Cellebrite
RESPONDER

Overview guide

May 2021 | Version 7.45

Cellebrite

Legal notices

Warnings

FCC WARNING: This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions:

1) This device may not cause harmful interference.

2) This device must accept any interference received, including interference that may cause undesired operation.

Contents

1. Introduction

Cellebrite Responder is an all-in-one forensics solution that helps speed the investigative process by extending logical data extraction capabilities to first responders, investigators, detectives and border/customs agents whenever and wherever it's needed.

Leveraging the trusted UFED platform, Cellebrite Responder features an intuitive interface which makes extracting live device data simple, saving time while ensuring strict access control. Cellebrite Responder is a multi-platform system that is designed to unify workflows between the field and lab, making it possible to view, access and share mobile data via in-car workstations, laptops, tablets or a secure, self-service kiosk located at a station.

This manual is for the users (investigators) and administrators of Cellebrite Responder.

A selection of features that are included with Cellebrite Responder:

- **Logical and physical extractions:** Extract specific data from the widest variety of mobile devices, SIM cards or USBs by timeframe, data types or relevant persons.
- **Selective extraction:** Select and extract only the relevant data required based on time range or specific subject information (person, email, device).
- **Quick copy:** Copy only specific evidence from witnesses and/or victims devices, leaving personal data private.
- **Capture images:** Capture images using the UFED camera, or capture screenshots directly from the device.
- **Chat capture:** Chat Capture is an automated screen capturing process that allows users to extract and analyze selective chat conversations from third party application data.
- **Case ID:** Preconfigured permission management and case ID features to help control data access, case integrity and user management.
- **Easy device detection:** Identify devices using autodetect, search or manual selection.
- **Networked connectivity**: Share statistics, reports and raw mobile data with other authorized personnel across a local network.
- **Filters:** View and analyze data using simple data filters such as crime related watch lists, people and timelines.
- **Reporting:** Generate a report on all or filtered information.

1.1. Extraction types

Cellebrite Responder includes a range of data extraction types.

The available extractions may vary, based on the type of product purchased; the Cellebrite Responder Logical or the Cellebrite Responder Ultimate product.

Table 1-1: Functionalities of the Cellebrite Responder products

Functionality	Cellebrite Responder Logical	Cellebrite Responder Ultimate
Logical Extraction	Yes	Yes
SIM Data Extraction	Yes	Yes
Password Extraction	Yes	Yes
Clone SIM	Yes	Yes
File System Extraction	Not available	Yes
Physical Extraction	Not available	Yes
Capture Images/Screenshots	Optional	Yes
Chat capture	Yes	Yes

The extraction types are:

- **Logical extraction:** Extracts user data from a mobile device (SMS, call logs, pictures, phonebook, videos, audio, certain application data, and more). Quickest extraction method but least amount of data.
- **SIM card extraction:** Extracts data from a SIM or USIM card.
- **File system extraction:** Extracts files embedded in the memory of a mobile device. Retrieve the artifacts within a Logical extraction, in addition to hidden system files, databases and other files which were not visible within a logical extraction.
- **Password extractions:** Unlocks and displays passwords from a source mobile device.
- **Clone SIM:** Copies a SIM ID from one SIM card to another SIM card or to a Cellebrite UFED SIM ID Access Card.
- **Physical extraction:** Extracts a physical bit-for-bit image of the flash memory of a device, including the unallocated space using advanced methods. Unallocated space is the area of the flash memory that is no longer tracked by the file system, which may contain images, videos, files, and more.

- **Capture images and screenshots:** Take pictures or videos of a device using the Cellebrite UFED camera. You can also capture internal screenshots directly from the connected device.
- **Chat capture:** Chat Capture is an automated screen capturing process that allows users to extract and analyze selective chat conversations from third party application data.

1.2. Accessories

- **UFED Device Adapter**: Connect this adapter to the Source Device port for device extraction via USB, RJ45, SIM Clone, and SIM extraction.

> The UFED Device Adapter is built in and is not required if you are using the Kiosk provided after June 2016.

The device adapter has the following connectors for source devices:

- SIM card reader
- USB port
- RJ45 port

Each connector has a LED that indicates availability during an extraction and blinks to indicate where to connect the source device. In addition there are LEDs for power and Bluetooth.

» **Multi SIM Adapter:** Universal adapter for Nano SIM, Micro SIM and SIM card cloning and extraction.

» **Accessories, cables and tips:** A selection of common accessories, cables and tips are located in the UFED cable kit attached to your Cellebrite Responder package.

1.3. Cellebrite UFED Device Adapter with USB 3.0

The Cellebrite UFED kit contains a device adapter that attaches to your PC's USB ports. Each connector has a LED that indicates availability during an extraction and blinks to indicate where to connect the source device. In addition, there are LEDs for power and Bluetooth.

Depending on when you received your kit, there are two types of device adapters: Cellebrite UFED Device Adapter with USB 3.0 (latest version) and Cellebrite UFED Device Adapter with USB 2.0 (previous version). This document provides more information on the Cellebrite UFED Device Adapter with USB 3.0.

This manual is also relevant for Cellebrite Responder users.

Some devices can be extracted only by using the Cellebrite UFED Device Adapter.

The Cellebrite UFED Device Adapter is built in and is not required if you are using the Kiosk.


UFED Device Adapter
Cellebrite
BLUETOOTH
GPIO
SERIAL
USB

This device adapter has the following connectors:

- GPIO port (for future use)
- USB 3.0 port
- RJ45 port
- DC In power supply (Input 5.3V 3.7A)
- 2 USB connection cables labeled POWER and DATA.

For information on the specifications, refer to the *Overview Guide*.

To connect the Cellebrite UFED Device Adapter with USB 3.0:

1. First connect the DATA cable to a USB port on the computer.
2. Then connect the POWER cable to a second USB port on the computer.

Use the following procedure, if the computer is mounted in a difficult to access or distant location.

To connect the Cellebrite UFED Device Adapter with USB 3.0 using extension cables:

1. Connect the Active Extension cable[1] to the DATA connection cable. Refer to the *Overview Guide*.
2. Connect the other end of this extension cable to a USB port on the PC.
3. Connect a standard USB extension cable to the POWER connection cable.
4. Connect the other end of this extension cable to a USB port on the PC.

1.3.0.1. Using the External power supply

The external power supply is NOT required for the smooth operation of the Cellebrite UFED Device Adapter V3, but is provided for those cases where additional power output is required. The external power supply provides an output of approximately 5.3V 2.7A.

[1]This cable is 150 cm in length and allows for the easy and accessible placement of the UFED Device Adapter with USB 3.0.

1.4. Using cables and tips

The cables and tips include various adapter cables (the number of cables depends on the Cellebrite UFED product and kit purchased). Each cable has a letter and name for example: A Adapter – USB.

Figure: Single cable

For easy recognition, the tips are color coded and numbered; the color represents the vendor.

Figure: Cellebrite UFED tip (example)

Before each extraction, the required cable and tip number and color is specified in the **Source** area of the Select Content Types screen.

1.5. Cellebrite YouTube channel

For your convenience, a selection of useful videos demonstrating typical workflows and common procedures are available at youtube.com/cellebriteufed.

1.6. Hardware specifications

Cellebrite Responder can be run on a kiosk as well as other platforms (see Using Cellebrite Responder on other platforms (on page 20)). This section provides information on the latest hardware (v7460) specifications of the Kiosk:

Computer	
All-in-one PC	Dell OptiPlex 7460
Processor	Intel i7-8700
Memory	Memory 32 (2x16) GB DDR4
Storage	1 TB SSD class 40
Screen	23.8 FHD (1920 x 1080), Touch Screen
Network	Intel® I219-LM Ethernet LAN 10/100/1000
Input/Output	External USBs: 1 x USB 3.1 Type C Gen 2 (side) 1 x USB 3.1 Type A Gen 1 with PowerShare (side) 4 x USB 3.1 Type A Gen 1 (rear) 1 SD Slot (side) 1 Universal Audio Jack (side) 1 DisplayPort Out (rear) 1 HDMI In (rear on Full HD only) 1 HDMI Out (rear) 1 Audio Line-Out (rear) 1 RJ-45 (rear) 1 Power Connector (rear)
Base	
SD Card reader	Cellebrite (1xXD, 1xmicroSD, 1xUDMA\CD\MD, 1xM2\MS\DUO)
SIM reader	Includes the UFED Device Adapter, support SIM via Source Device USB port

DVD/Blu-ray	N/A
Input/Output	5 x USB 1 x RJ45

Kiosk supports standard Windows programs.

Compatible accessories: UFED Camera, UFED cables and tips.

1.7. Using Cellebrite Responder on other platforms

Cellebrite Responder can be run on a kiosk as well as other platforms. This section provides information on installing Cellebrite Responder on a workstation, laptop or tablet:

» Minimum requirements (below)
» Installing the application (below)

1.7.1. Minimum requirements

The minimum requirements for a workstation, laptop or tablet to run Cellebrite Responder are as follows:

PC	Windows compatible PC with a Pentium IV or compatible processor running at 1.6 GHz or higher
Operating System	Microsoft Windows 10, 64-bit Microsoft Windows 8.x, 64-bit Microsoft Windows 7, 64-bit
Memory (RAM)	16 GB (32 GB recommended)
Screen resolution	1024 X 768 or higher
USB ports	4 x USB ports (USB 2.0 or higher)
Hard drive	500 GB
Optional	Web camera or UFED Camera

1.7.2. Installing the application

To install Cellebrite Responder on a workstation, laptop or tablet:

1. Obtain a copy of the Cellebrite Responder application.
2. Double click the Cellebrite Responder .exe file.
3. Follow the installation wizard to install the application.

2. Getting started

This section explains the following:

2.1. Logging in

To start the application:

1. The first time that you start Cellebrite Responder it will prompt for license information (see Activating the license (on page 24)).
2. After the license is activated the Home screen appears (see Using the Home screen (on page 30)). The Home screen will also appear when you restart the kiosk.

> If the Cellebrite Responder administrator has added user credentials to the system the Login window appears.

3. Enter your credentials to log in.

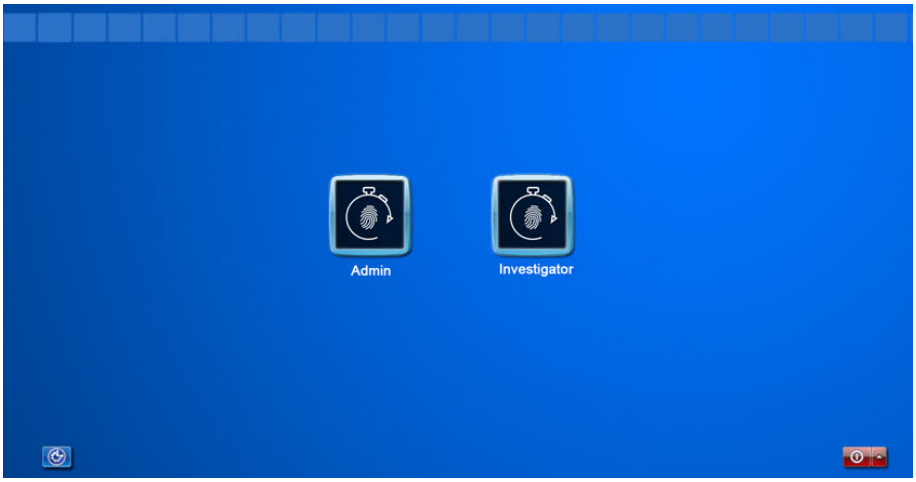
> Admin and user credentials are specified in Cellebrite Commander or UFED Permission Manager. *See* Using the Cellebrite UFED Permission Manager (on page 127).

2.1.1. Logging in as an administrator

By default, the kiosk starts in investigator (or user) mode. The following procedure is applicable to the kiosk version.

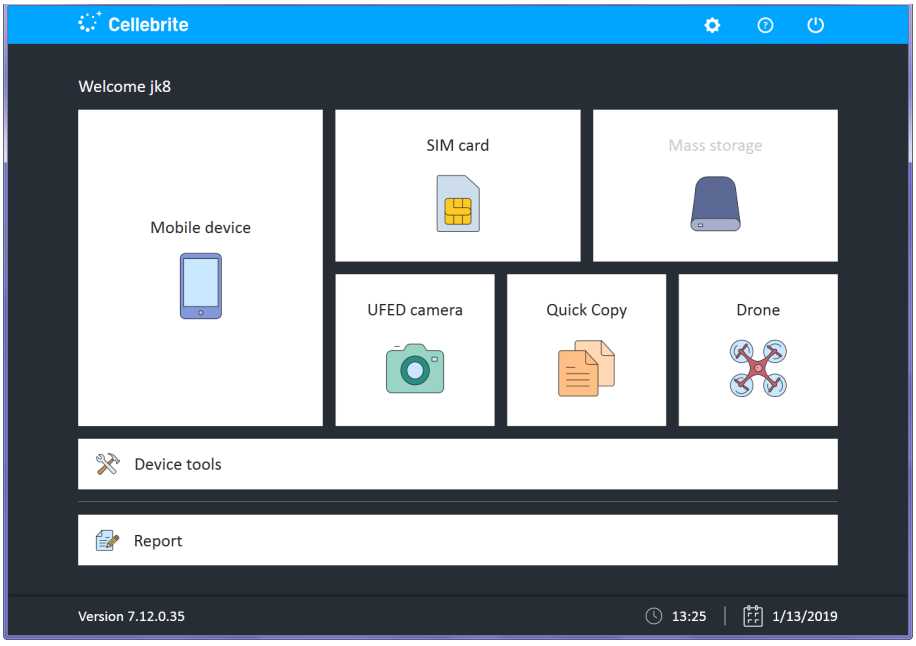
To log in as an admin:

1. Press Ctrl+ALT+Delete and select **Log off**. The following window appears:



2. Tap **Admin** and then enter the default admin password. To obtain the password, contact Support.

   The Cellebrite Responder Home screen appears and the **Settings** button is now available.



To access the Windows desktop press ⊞Win+D buttons.

2.2. Activating the license

Activate Cellebrite Responder in one of the following ways:

- Using a dongle license (on the next page)
- Using a network dongle (on page 28)

Check your Cellebrite UFED kit to make sure which method you should use.

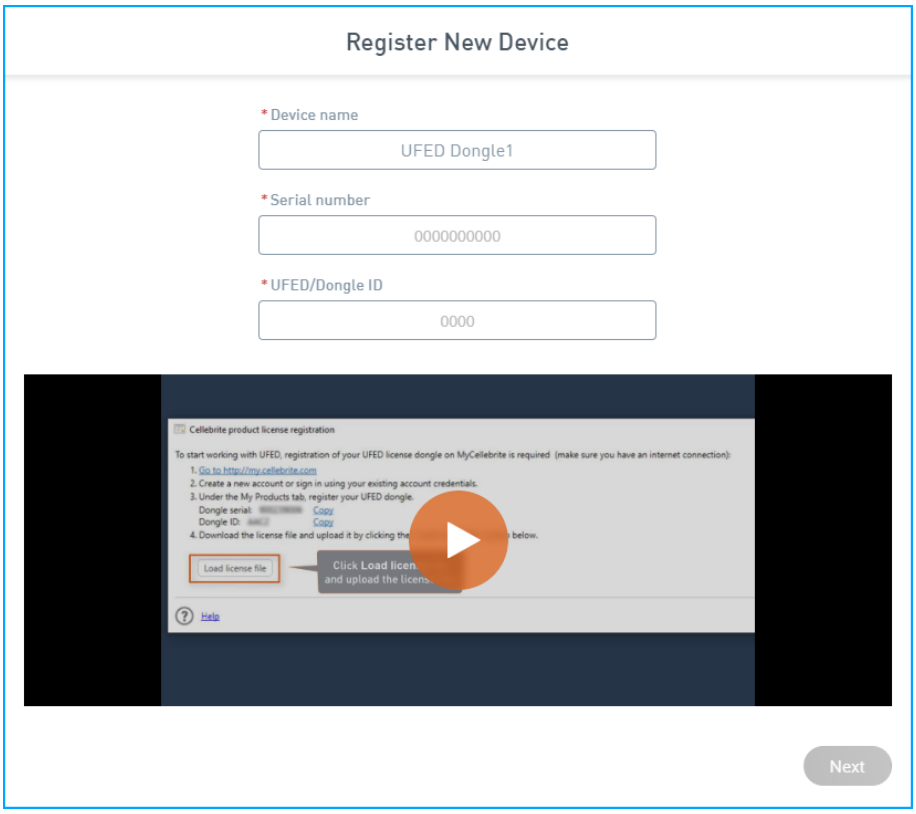
If you are using Cellebrite Responder for the first time or a license is not found, see License not found (on page 96).

2.2.1. Using a dongle license

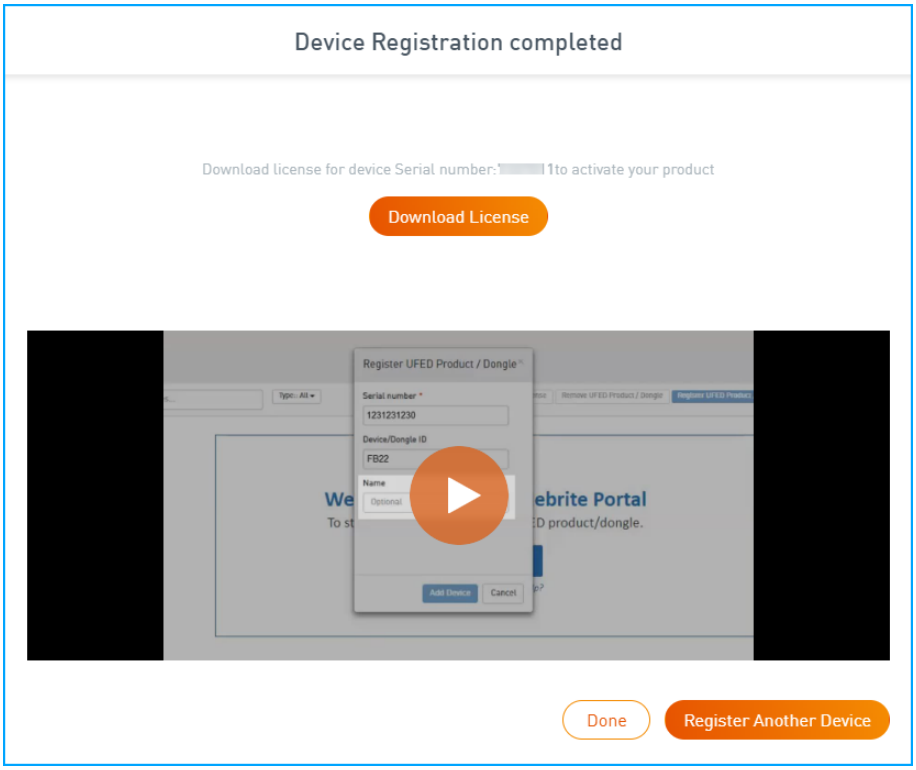
Use the Cellebrite UFED dongle provided with your Cellebrite UFED kit. The dongle contains licenses for all the applications purchased.

To use Cellebrite Responder with a dongle:

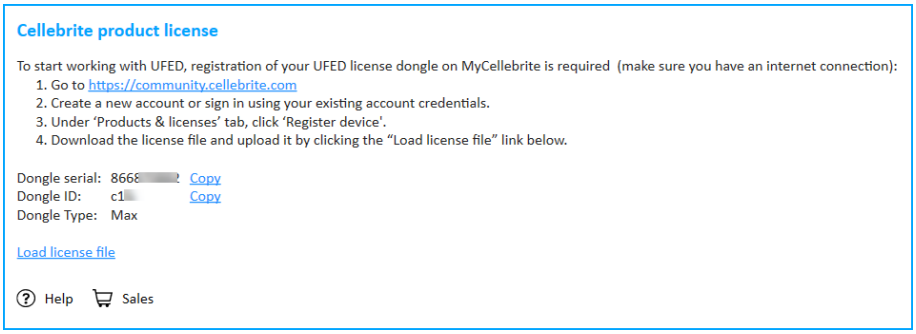
1. Go to community.cellebrite.com and log in with your credentials (or create an account).
2. Go to **Products & Licenses** > **Register Device** and enter a name for the device, the serial number and Dongle ID as displayed on the dongle.



3. Click **Next**. The following window appears.



4. Click **Download License** from the Device Registration Completed window to download the license key (or click **See licenses** in the Products tab and then from the menu on the right select **Download license**).
5. Download and install the Cellebrite Responder application.
6. Start the Cellebrite UFED application and connect the dongle to a USB port on your computer. The following window appears.

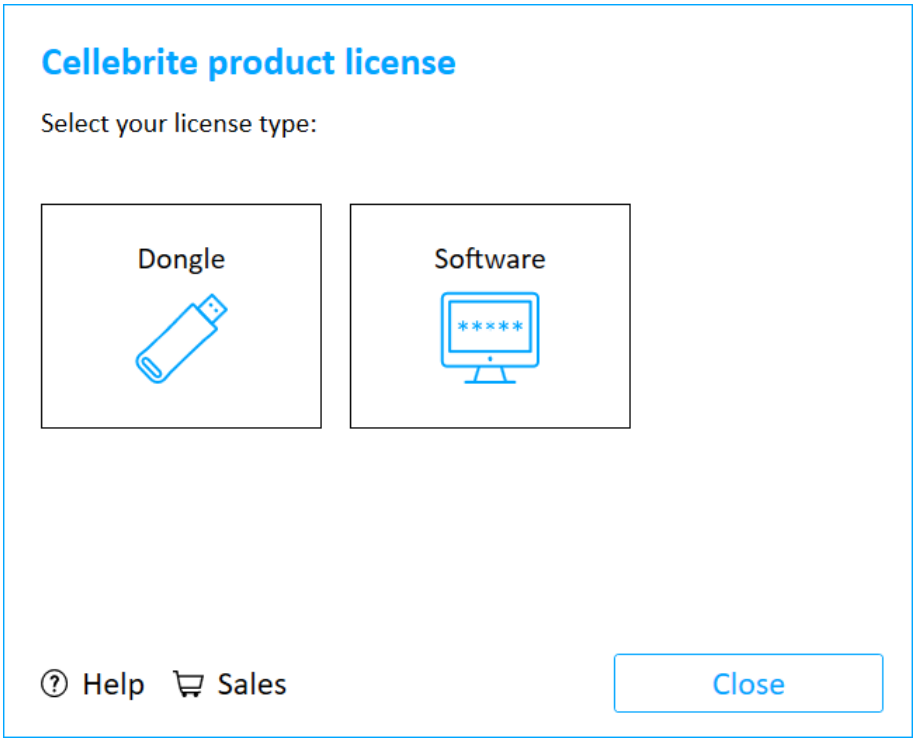


7. In the Cellebrite product license window, click **Load license file** and upload the license key.

   Congratulations, your Cellebrite Responder application is now ready!

If a license dongle is not found:

1. When a license dongle is not found, the Cellebrite product license window appears.



2. Tap **Dongle**. If you connected the dongle to a USB port on your computer, and it still does not work, contact support@cellebrite.com.

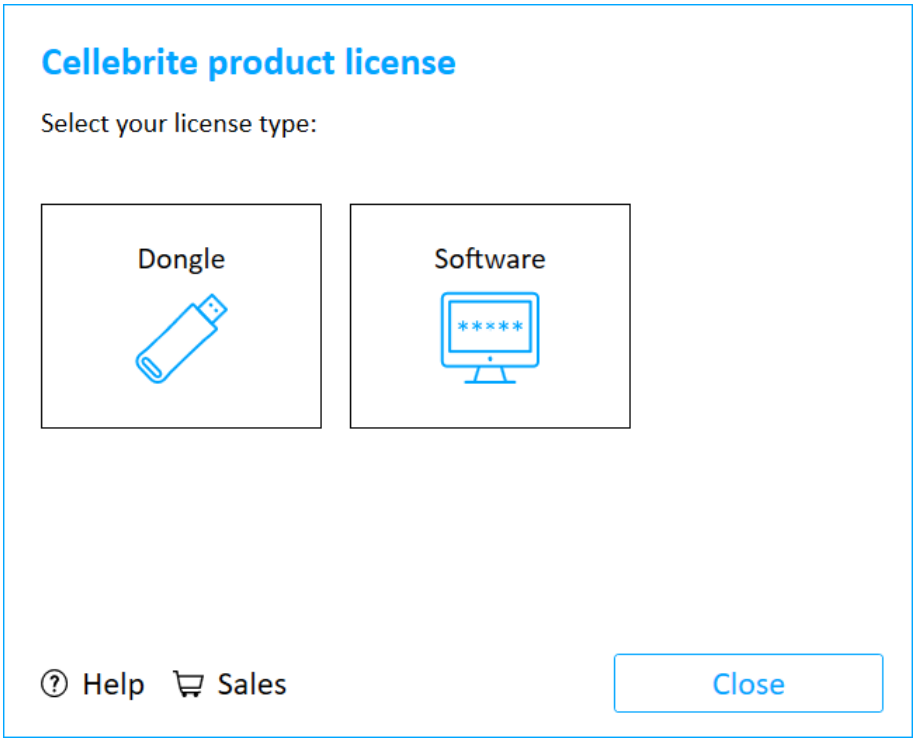
2.2.2. Using a network dongle

The network dongle is connected to your organization's network and contains licenses for all the applications purchased.

To use Cellebrite Responder with a network dongle:

If a network dongle is not found:

1. If the network dongle is not recognized, the Cellebrite product licensing window appears.



2. Tap **Network**. The following window appears.

> If a dongle was not found on the network. Make sure that you have an Internet connection and that a dongle is connected to the network. Then tap **Refresh** to search for a network dongle again.

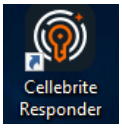
> If you tap **Refresh** twice, a new window will appear where you can manually connect to the network dongle. Tap **Advanced** and then enter the IP address (or host name).

> If there is only one network dongle it will be selected automatically. If there are multiple network dongles, select the required Dongle Serial number.

Congratulations, your Cellebrite Responder application is now ready!

2.3. Starting the application

When you turn the kiosk on, the Cellebrite Responder application starts automatically and the Home screen is displayed.

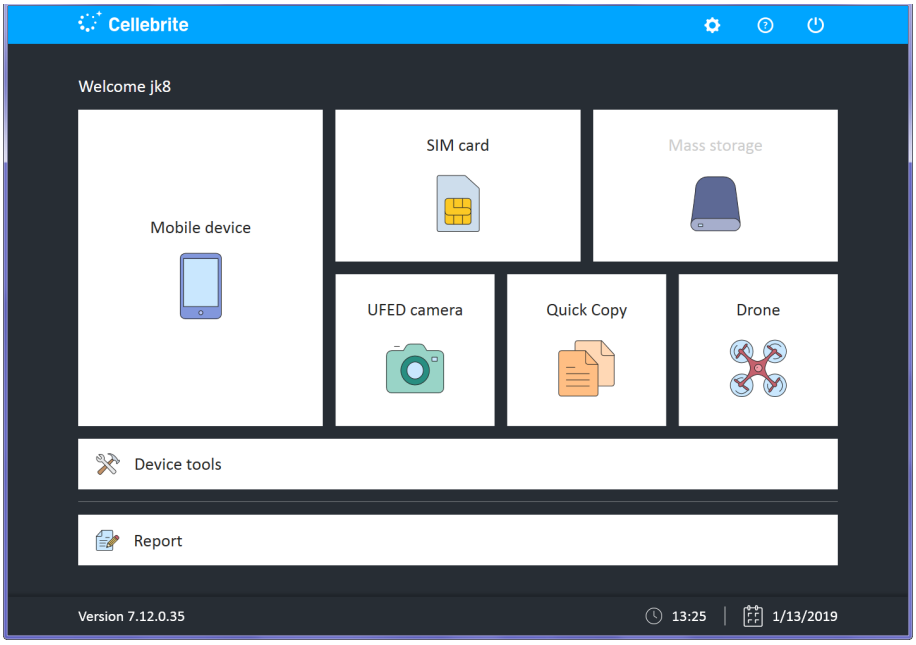
If you are running Cellebrite Responder on a workstation, laptop or tablet, double-click the 

shortcut on your desktop. For information on the Home screen, see Using the Home screen (on the facing page).

2.4. Using the Home screen

The Home screen groups the extraction data into distinct areas: Mobile device, SIM card and USB device. In addition, users can directly operate the camera for immediate image capturing or access the device tools. All extraction functionality is driven by **automatic** identification of the device, or by **searching** for the device. Cellebrite Responder determines what functions are available for the specific device and displays the relevant functions.

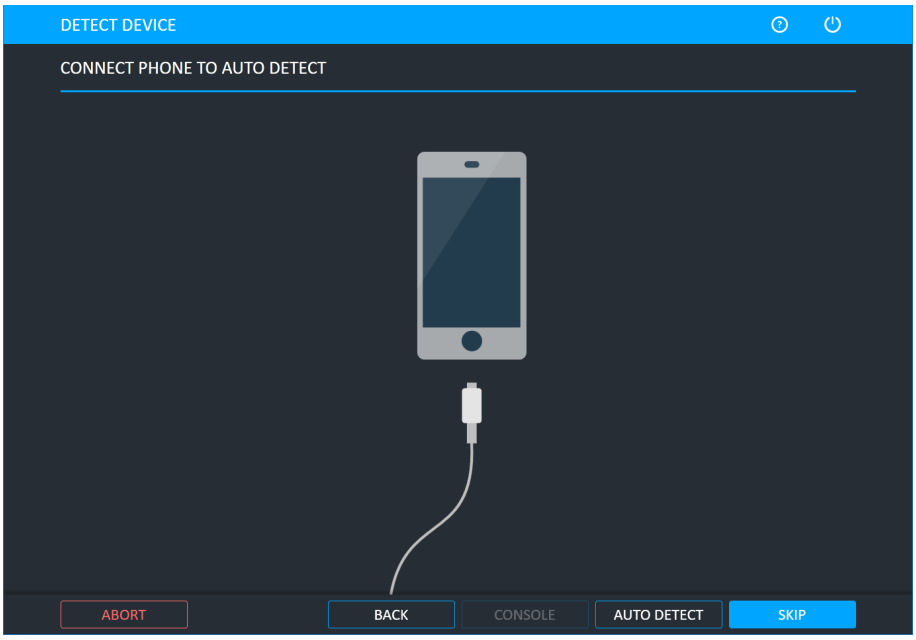
The Home screen is displayed next.



2.5. Autodetecting a device

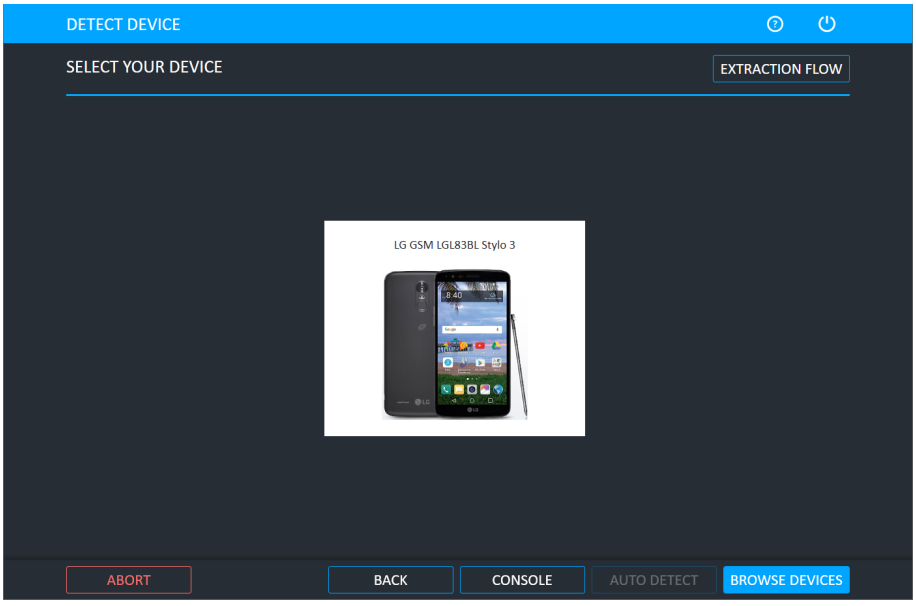
To use Autodetect to locate the mobile device:

1. Connect the mobile device to the Cellebrite Responder unit.

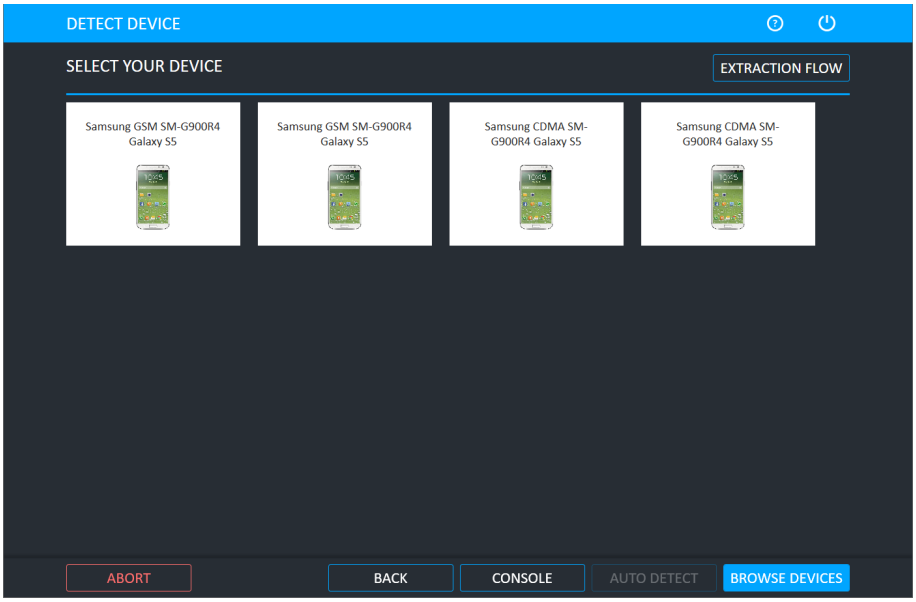


2. Select **Auto Detect** at the bottom of the screen.

   If the connected device is recognized by the system the following window appears.



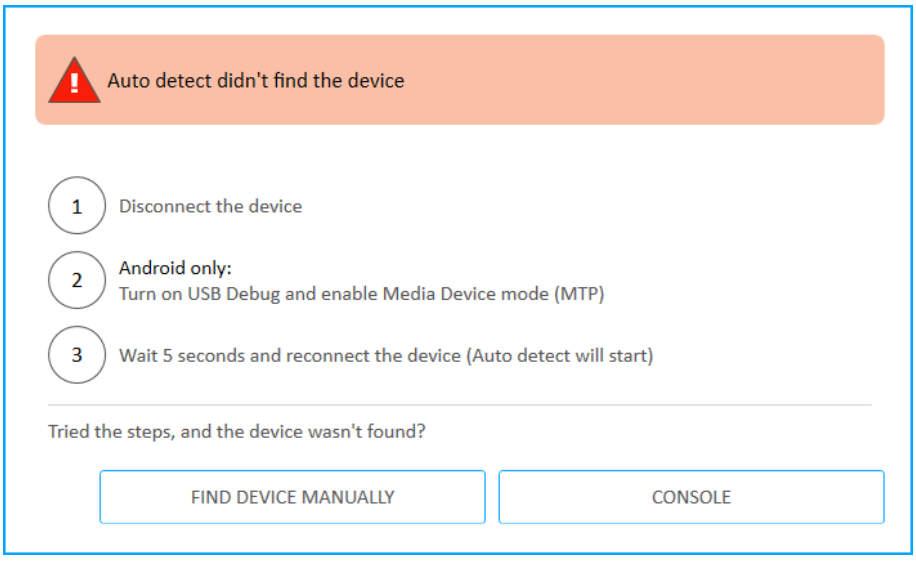
If multiple matches are found, the following window appears.



3. Select the relevant device.
4. Alternatively, tap **Browse Devices** to manually search for the device.

> Click the **Console** button to access device information using the Android Debug Console. For more information, refer to the *Performing extractions* manual.

5. If the connected device cannot be recognized by the system, a message prompts you to try the following steps or tap Find device manually.

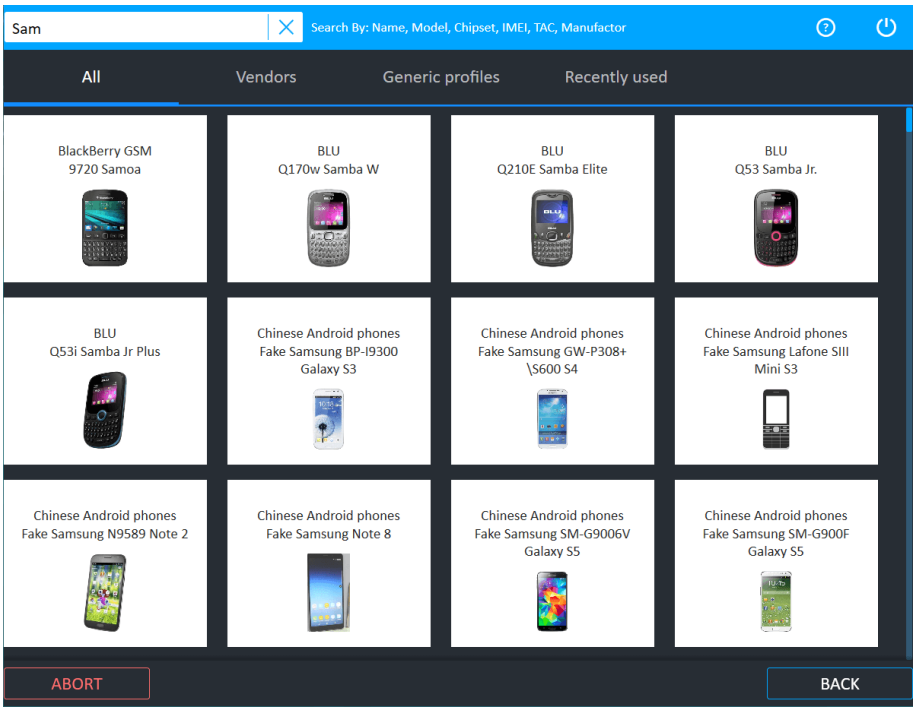


6. If the device still cannot be found, tap **Browse Devices** or **Console**.

2.6. Searching for a device

To search for the mobile device:

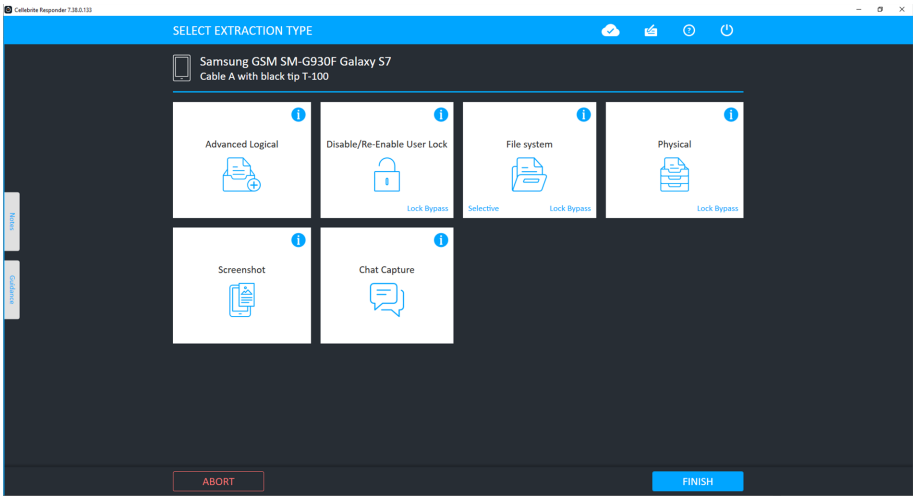
1. Narrow the list by vendor, recently used, etc. or begin typing in the search box in the top bar to search for a device or model. As you type, the list of devices is reduced to match your search criteria.



> You can also search for a device by its IMEI value, which is used to uniquely identify devices. The IMEI value is usually found printed inside the battery compartment of the device, or dial *#06# from the phone keypad. Enter the value in the search box, using a minimum of four digits up to the full number. If the IMEI value is recognized, matching devices will be displayed.

2. Select the device model type from the list.

Having selected the **device**, Cellebrite Responder will determine what extraction functions are available for this combination and present those functions as follows:



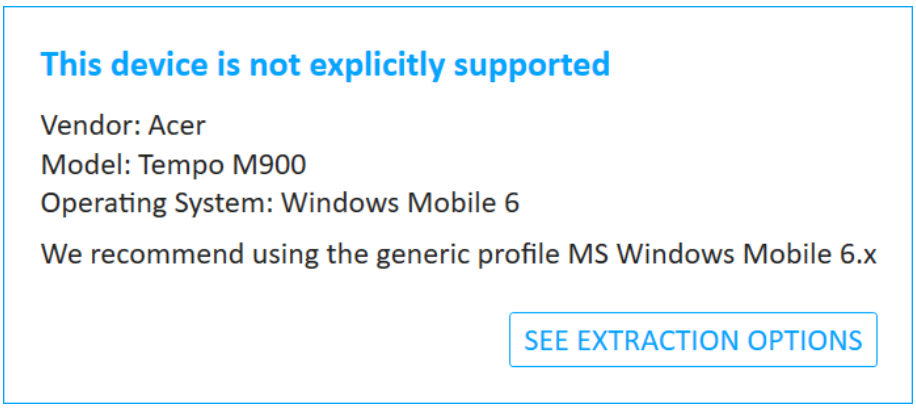
Lock Bypass is displayed for both physical and file system extraction methods that can bypass the user lock of the device.

2.6.1. TAC search

If you cannot find the Android device which you are looking for after performing a TAC number search, a window will appear. This window appears if Cellebrite UFED does not support the device directly, but there are applicable generic options available for the device.

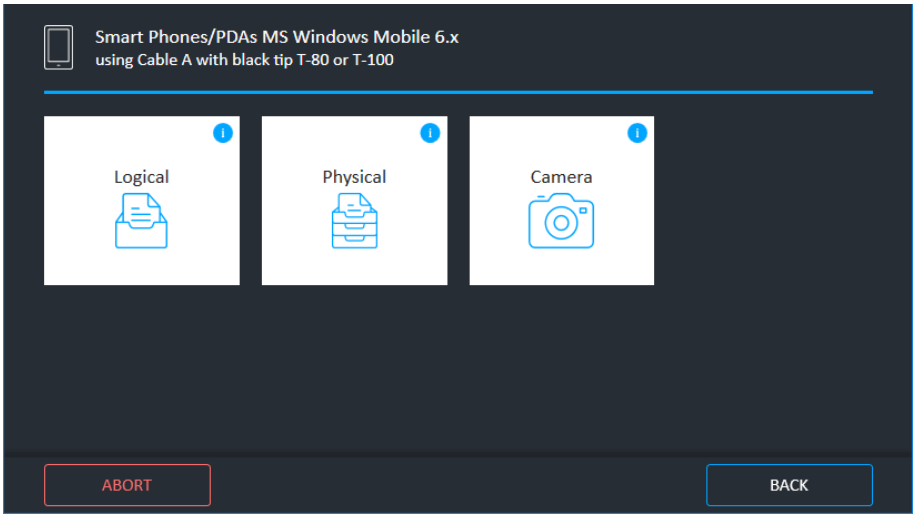
To retrieve device information and view generic extraction options:

1. Enter the complete 8-digit TAC number. The following window appears.

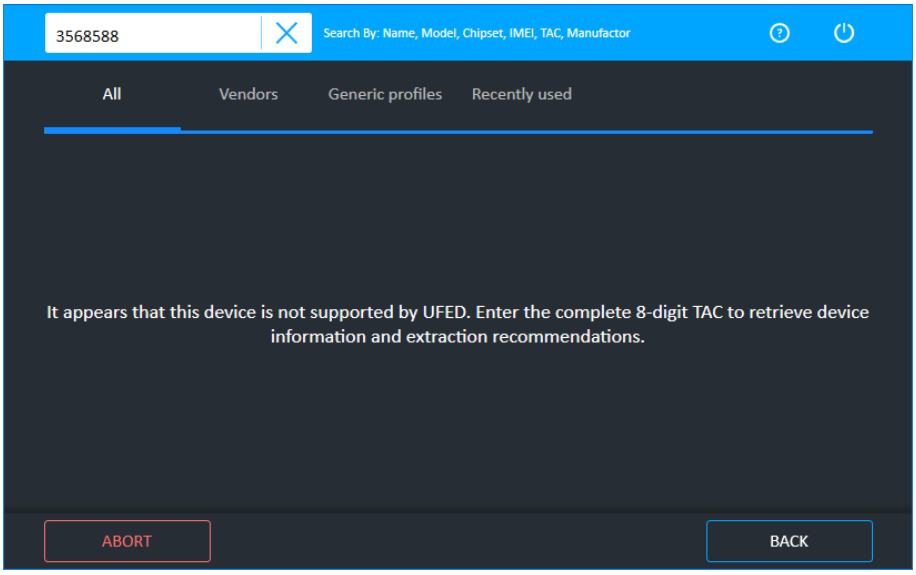


   The window includes the vendor, operating system and device name.

2. Tap **See recommended extractions**. A window appears with the generic extraction options for the device. An example appears next.



If you enter a partial TAC number (with less than 8-digits) or the device is not supported by Cellebrite UFED then the following window appears.



2.7. Case details

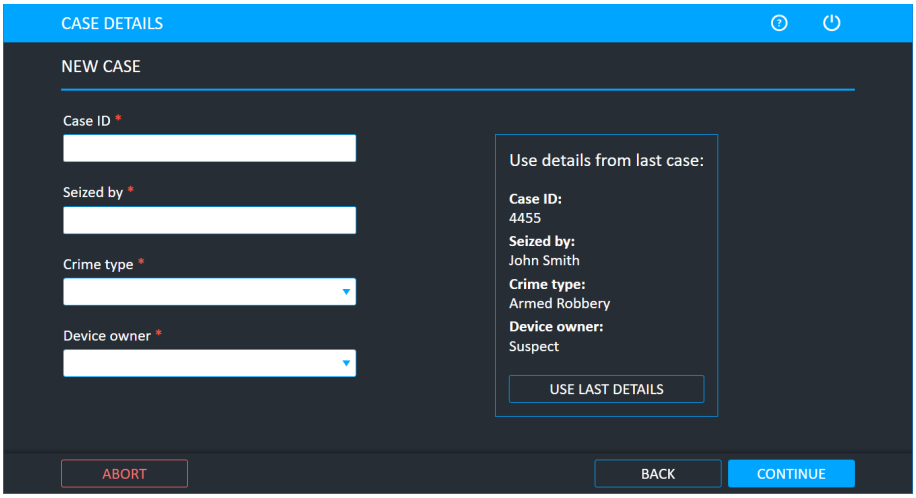
The Case details feature enables you to enter case details when performing an extraction or using the Cellebrite UFED camera. This feature is not enabled by default.

To enable the case details feature:

» Select **Include Case details screen** under **Settings** > **General**. For more information, see General settings (on page 80).

To specify the case details:

1. On the Home screen, select an extraction type or Cellebrite UFED camera. The following window appears.



2. Use the current case information, or enter and select the case information and then tap **Continue**.

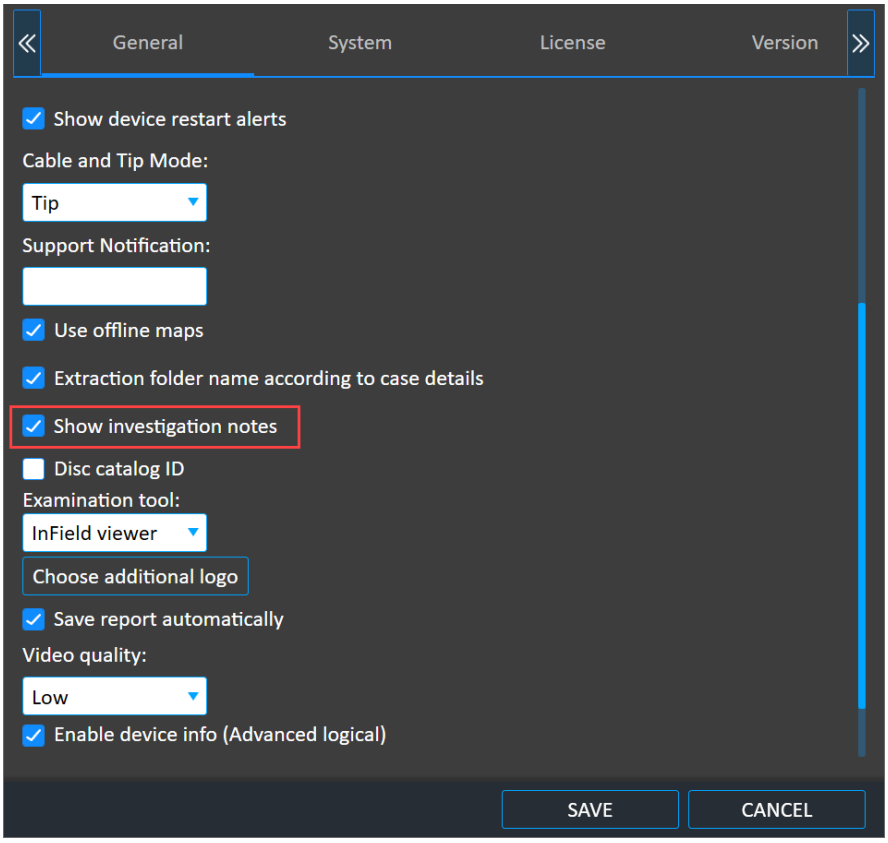
> The Crime Types list can be changed via the Cellebrite UFED Permission Manager (Using the Cellebrite UFED Permission Manager (on page 127)) or Cellebrite Commander (refer to the Cellebrite Commander manual).

2.8. Investigation notes

The Investigation notes feature enables you to add notes during the data extraction process. You can include observations or report any issues encountered during the process.

To enable or disable the feature:

1. Select **Settings** > **General**. The following window appears.



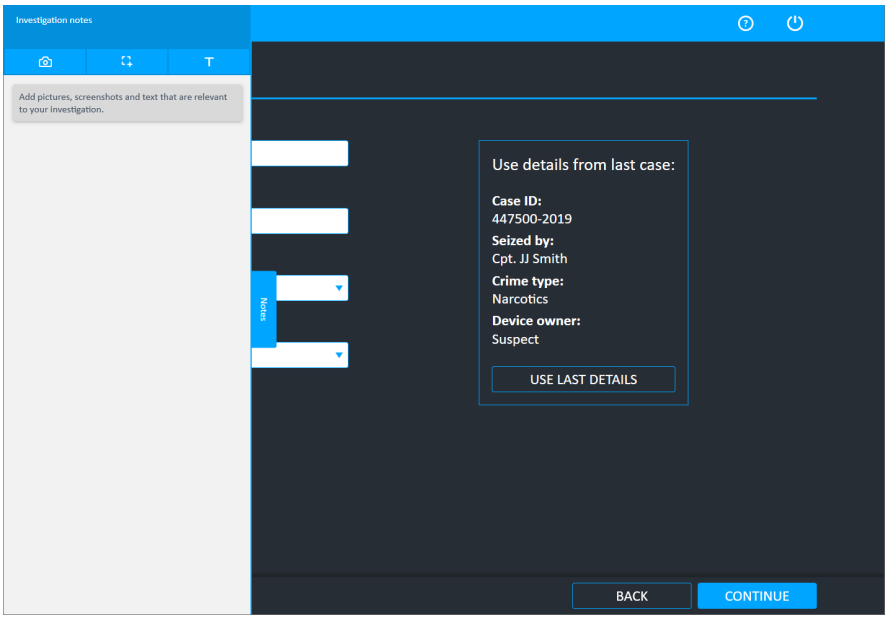
2. Select or clear the **Show investigation notes** check box.
3. Tap **Save**.

   This feature is enabled by default in Cellebrite Responder.

2.8.1. Using the feature

You can add pictures, screenshots and text that are relevant to your investigation to create an audit trail of actions taken and decisions made.

1. Start an extraction and tap **Notes**. The Investigation notes window appears.



   To close the window, tap the Cellebrite UFED interface outside of the Investigation notes window.

2. Add text, screenshots and pictures that are relevant to your investigation. The investigation notes are available as part of the extracted data or report. See Investigation notes (on the previous page)

See the following procedures to add text, screenshots and pictures:

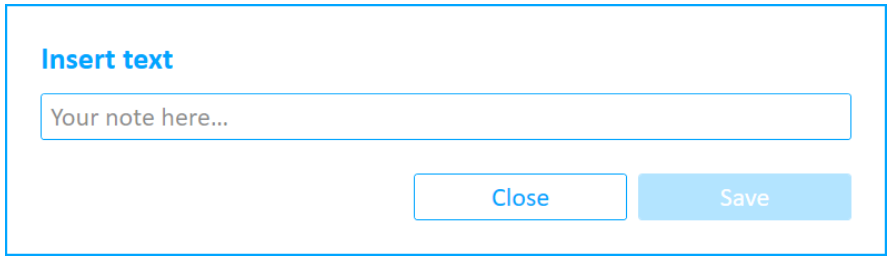
To add text notes: (on the next page)

To add screenhots: (on page 40)

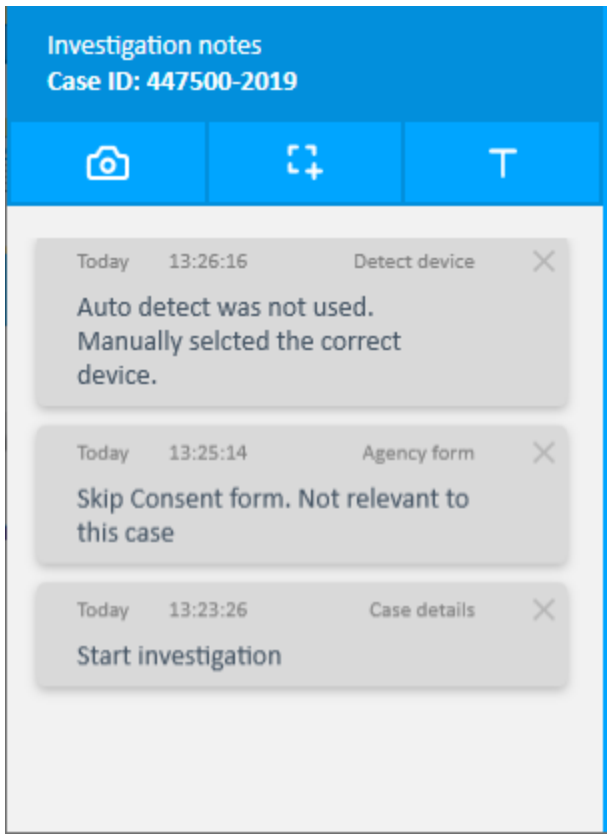
To add pictures: (on page 41)

To add text notes:

1. In the Investigation notes window tap Text ( ). The following window appears.



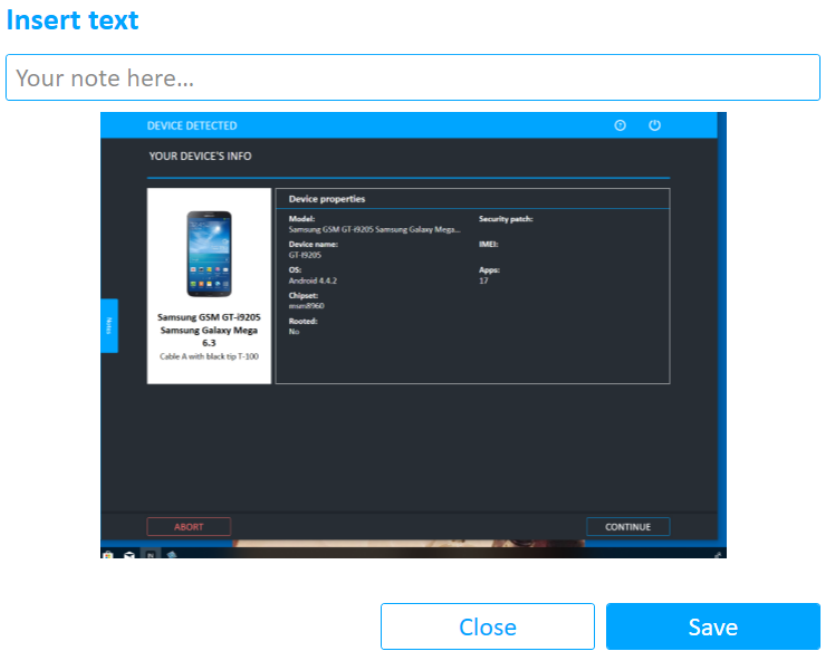
2. Enter the required text and tap **Save**.
3. The text is added to the Investigation notes panel and it includes the date, time and stage of the extraction process. An example is displayed next.



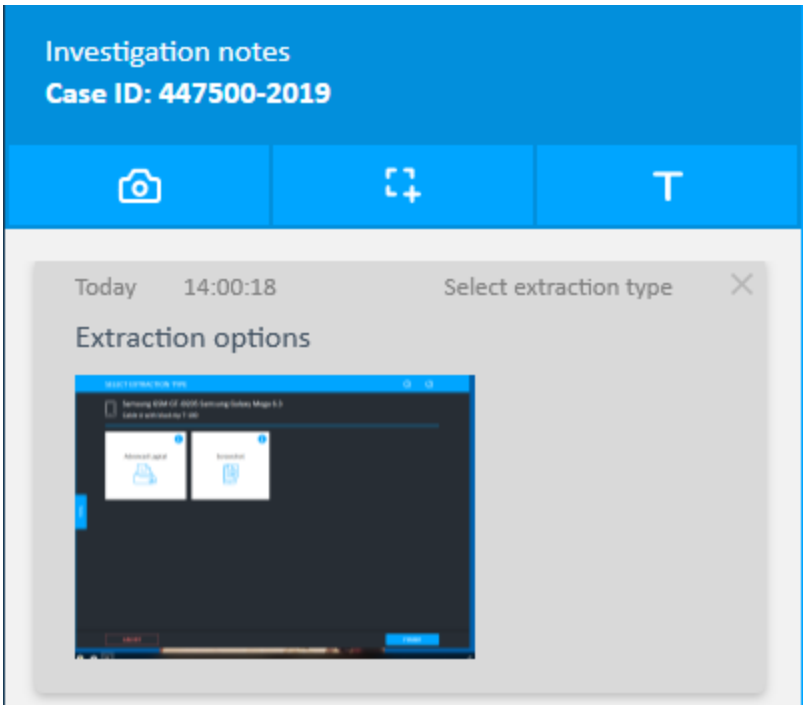
To remove a note tap Delete (X).

To add screenhots:

1. In the Investigation notes window tap Screenshot ( ). The following window appears.

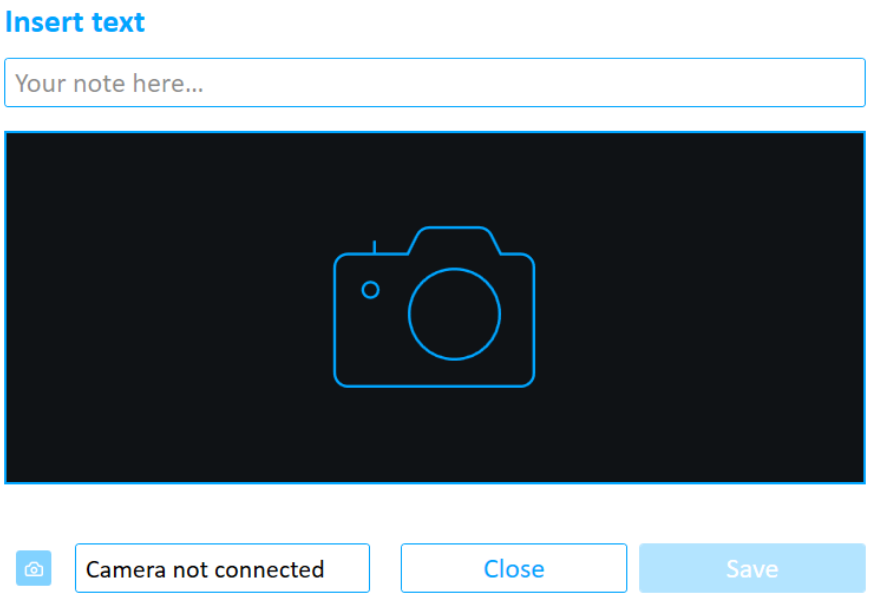


2. Enter the required text and tap **Save**.
3. The screencapture is added to the Investigation notes panel and it includes the date, time and stage of the extraction process. An example is displayed next.

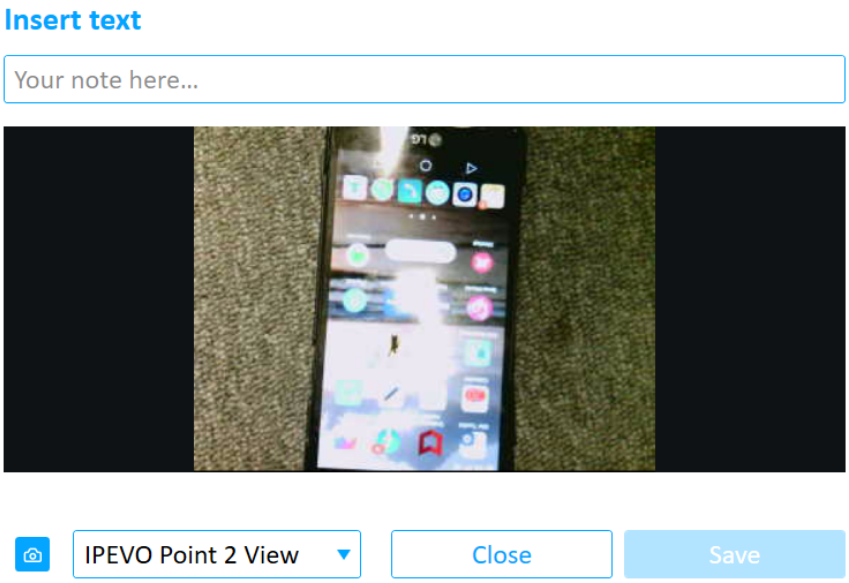


To add pictures:

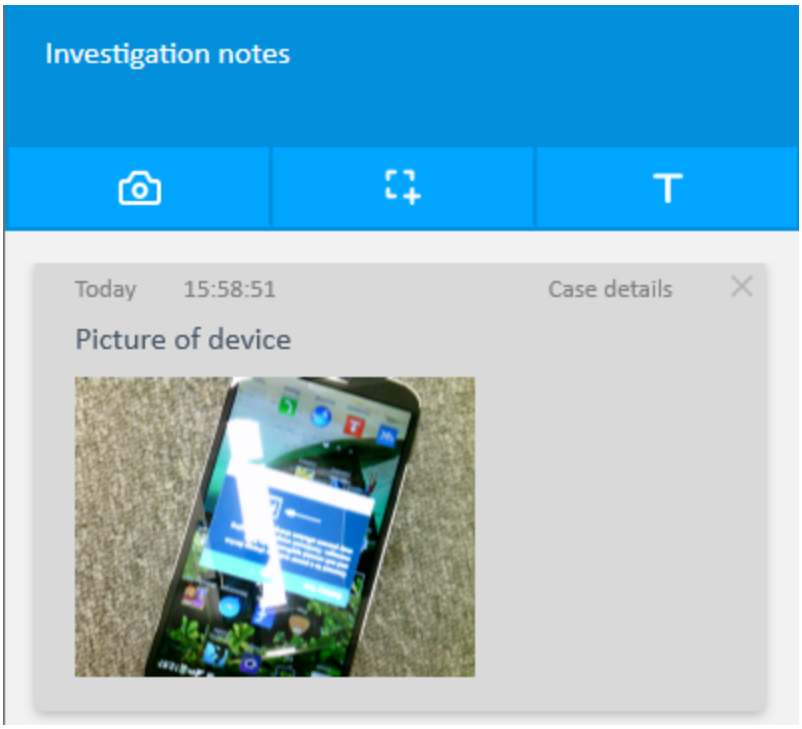
1. In the Investigation notes window tap Picture ( ). The following window appears if a camera is not connected.



2. Connect a camera to Cellebrite UFED.



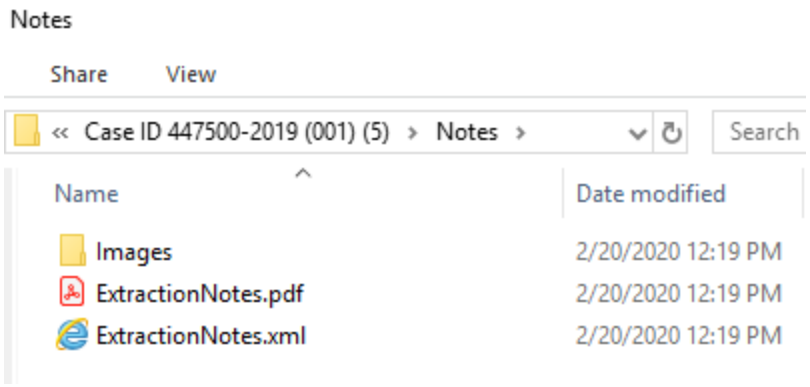
3. Select the required camera to use.
4. Tap Camera ( ) to take a picture. If required, tap Refresh ( ) to take a new picture, or tap Rotate to rotate the picture.
5. Enter the required text and tap **Save**.
6. The picture is added to the Investigation notes panel and it includes the date, time and stage of the extraction process. An example is displayed next.



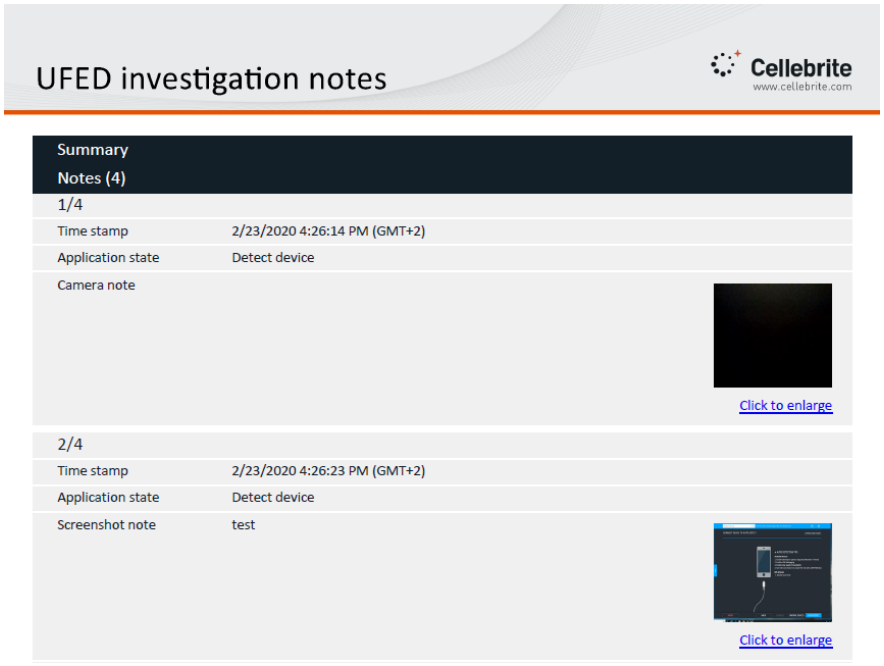
2.8.1.1. Accessing the extraction notes file

After completing the extraction, the investigation notes will be displayed as an ExtractionNotes.pdf file in the Notes folder when the report or extraction is saved.

Examples are displayed next.



Folder location



Example Investigation notes

2.9. Workflow guidance

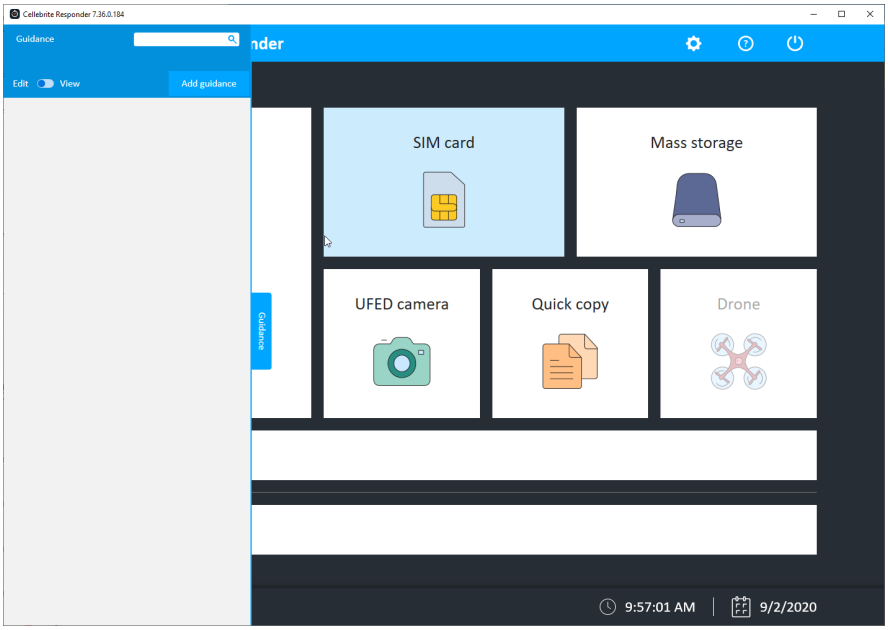
Workflow guidance allows admins to create guided instructions to assist users during the workflow. Workflow guidance can be made mandatory to ensure users read the guidance. To

manage Workflow guidance, see Workflow guidance settings (on page 139).

Creating Workflow guidance

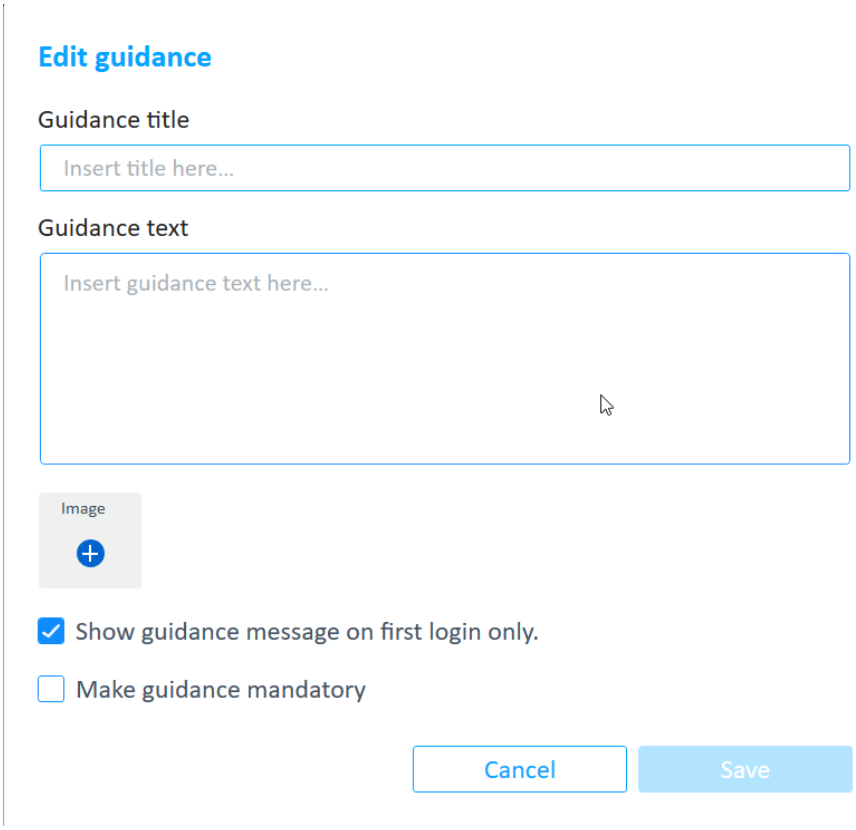
1. From the main screen, click the **Guidance** tab.

   The Guidance panel appears.



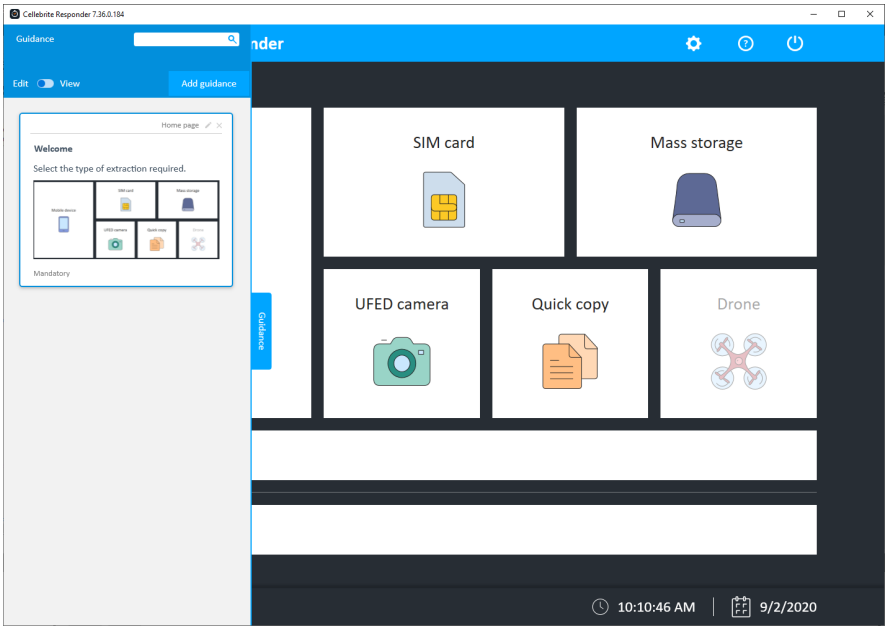
2. Click the toggle button to enable **Edit** mode.
3. Click **Add guidance**.

   The Edit guidance window appears.



4. Enter the guidance title and text.
5. Add an image (optional).
6. Select **Show guidance message on first login only** (optional).
7. Select **make guidance mandatory** (optional).
8. Click **Save**.

   The new guidance will appear in the Guidance panel.



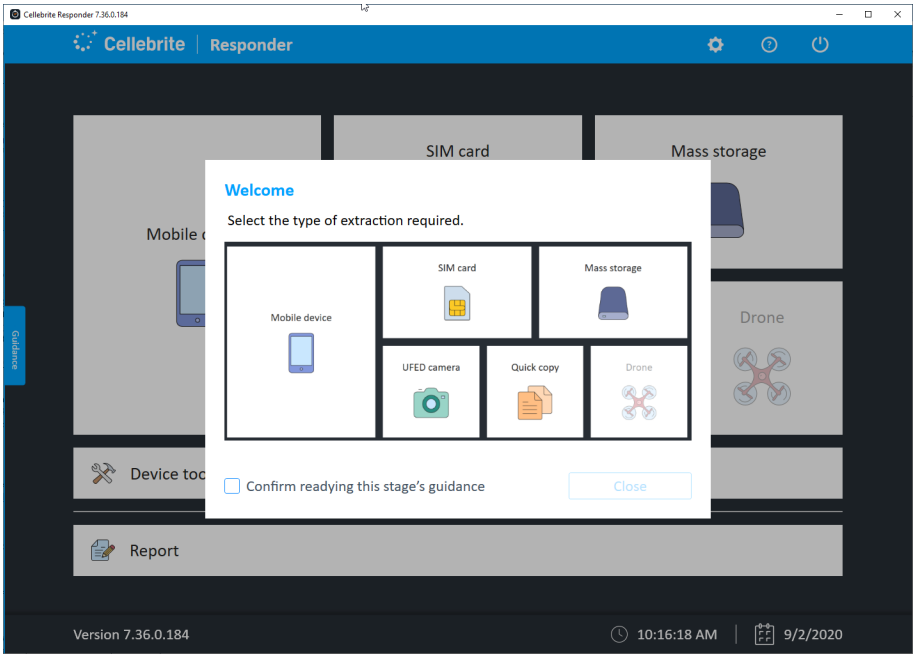
9. Continue adding the required guidance for each screen in the workflow. The guidance will appear on the screen from which it was created.

There can only be one guidance added to each screen.

Using Workflow guidance

The Workflow guidance added by the admin will appear during the workflow stages.

In the example below, the home screen guidance appears when opening Cellebrite Responder.



1. Review the guidance.
2. Check **Confirm reading this stage's guidance.**

> This will be displayed if the guidance was made mandatory by the admin in the Workflow guidance settings.

3. Click Close.

2.10. User predefined filter

The User predefined filter provides the ability to extract and view only a portion of the device content, based on time range or specific subject information (person, email, phone). This can be useful when:

- The agency has a warrant to extract data from a specific time window, and is not allowed to view additional data that is not covered by the warrant.
- The user wishes to save time and get to the relevant data ASAP.

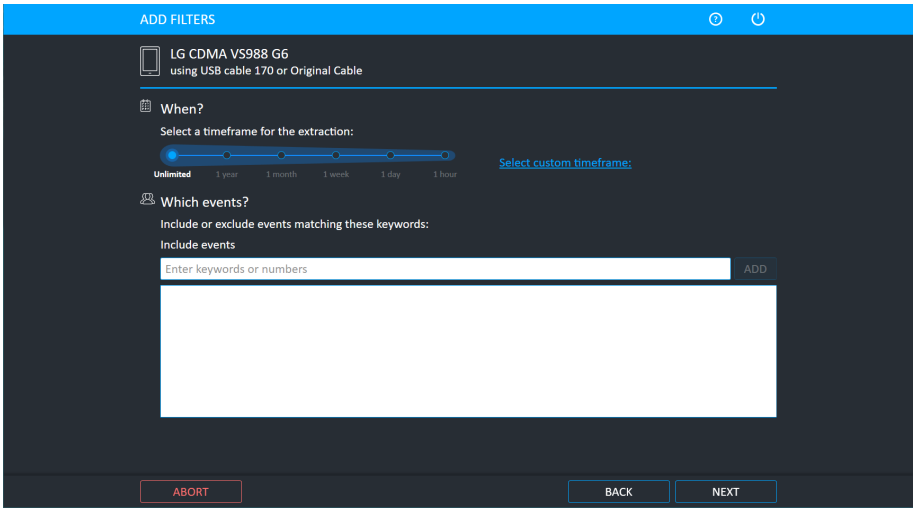
The most time consuming phase during a device extraction is transferring the data from the mobile device to the extraction tool. Timeframe filtering is performed on the device (when technically supported), and can reduce the extraction time. Another advantage is the reduced amount of data that the agent needs to browse through in order to find the evidence.

To enable the User predefined filter:

- Select **Allow user predefined filter** under **Settings** > **General**. For more information, see General settings (on page 80).

To specify the timeframe and parties for the extraction:

1. Identify the device and select an extraction type. The following window appears.



The extraction is based on the Cellebrite Responder unit's date and time. When selecting a time frame you should also consider the device's time zone.

The timeframe option is not applicable to file system extractions.

2. Select the required time frame. The less time selected, the quicker the extraction.
3. Enter keywords or numbers that you would like to include.

Selective extraction by party: Similar to the time frame, the ability to extract and review only data relevant to a specific party (number or device).

Partial numbers will be matched by the application, and names are matched irrespective to the capitalization.

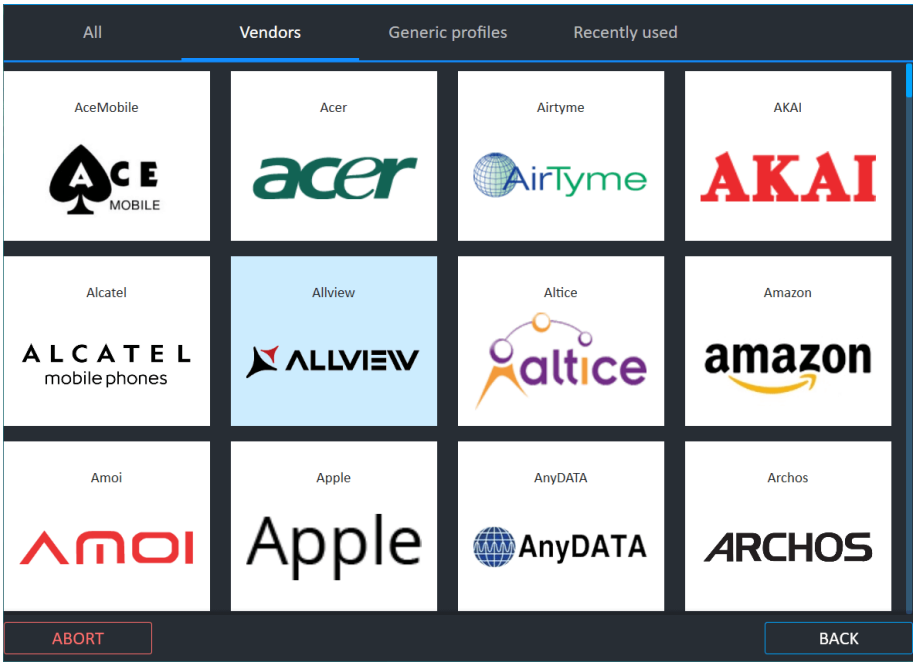
4. Tap **Next**.

2.11. Manual selection

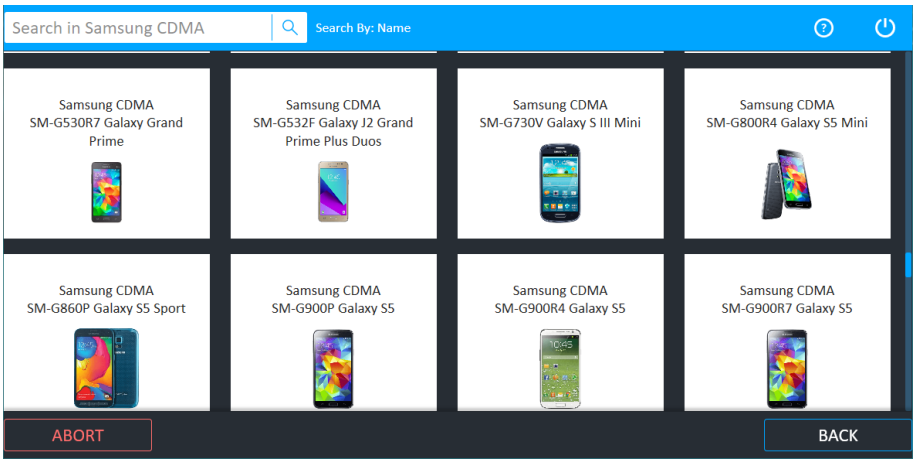
To manually select the vendor and model:

1. Tap **Mobile device** and then tap **Skip**.

   You can then select **All**, **Vendor**, **Generic profiles**, or **Recently used**. As displayed next, the Vendor screen enables you to select the device vendor.



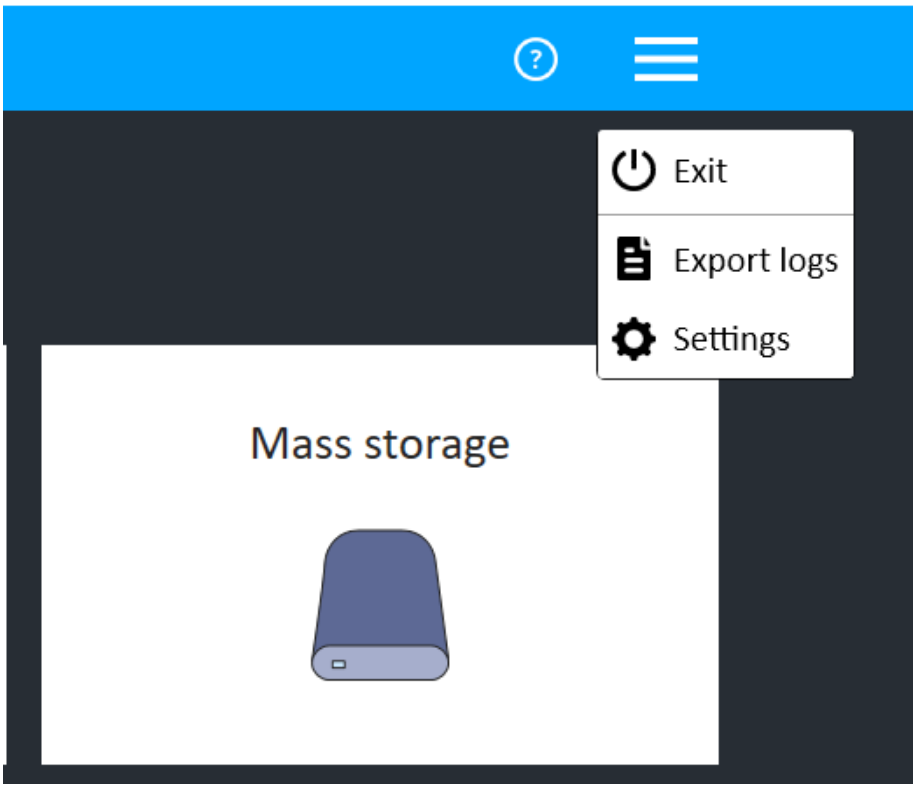
2. After choosing the Vendor, the application presents the Select Model screen where the specific model of the device is chosen:



   Having chosen the **Vendor** and the **Model**, Cellebrite Responder will determine what extraction functions are available for this combination and present those functions.

2.12. Application taskbar

The application taskbar is located at the top of the screen.



Application taskbar icons and descriptions

Icon	Description
	Click to select Online help or Extraction flows document.
	Click the menu icon to access the following: » Exit » Export logs » Settings

2.13. Virtual keyboard

The virtual keyboard allows you to type text whenever needed.

Figure: Virtual keyboard

- To show the virtual keyboard, double-tap any text box requiring input.
- To close the virtual keyboard, tap the X icon in the top right corner of keyboard panel.
- To show or hide the on-screen keyboard, select or clear the **Show on screen keyboard** check box under **Settings** > **System**. This check box is selected by default.

Table: Virtual keyboard icons and descriptions

Icon	Key Function
&123	Switch to numbers and symbols mode
↵	Create a new line
⌫	Delete the last character
↑	Activate CAPS LOCK

Any external USB keyboard can be connected to a USB port in the back panel, or a Bluetooth keyboard paired with the Bluetooth interface of the device.

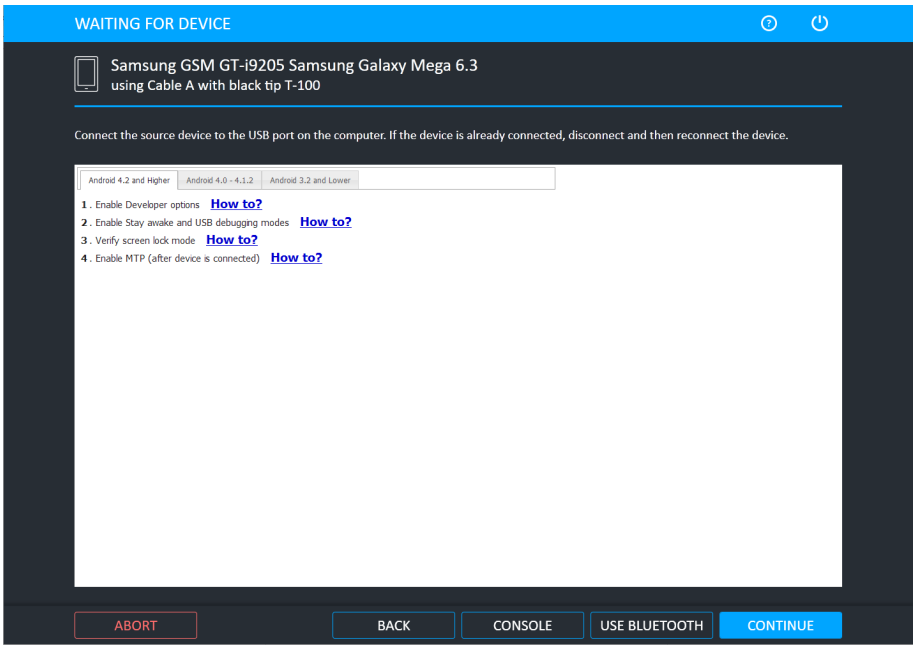
3. Advanced logical Android extraction

The following procedure explains the Advanced logical extraction process for an example device. The procedure may vary depending on the selected device. This section shows only one of the many extraction types that can be performed.

To perform an Advanced logical extraction from a mobile device:

1. Tap **Mobile device** and identify the device, then tap **Advanced Logical**.

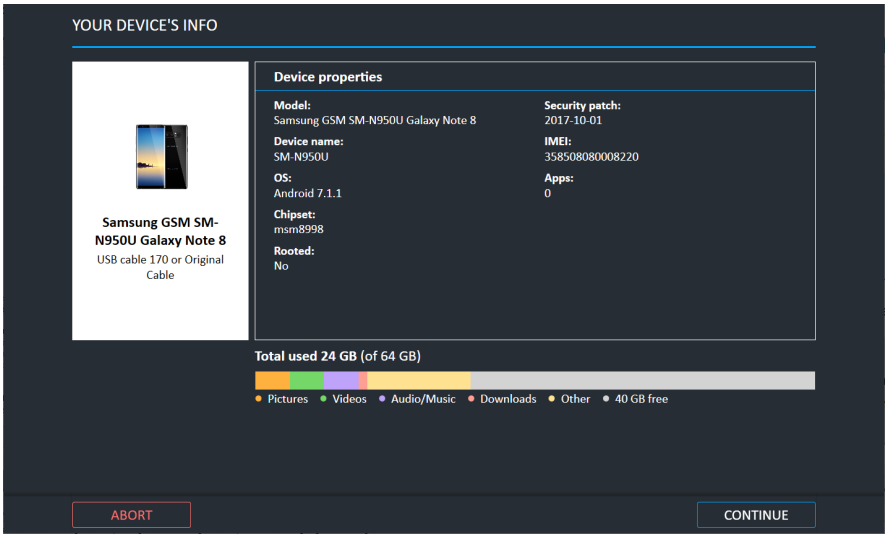
> For information on using optional timeframe and party filters, refer to the *Overview Guide*.



> Click the **Console** button to access device information using the Android Debug Console. For more information, refer to the *Performing extractions* manual.

2. Select the correct cable and tip for the mobile device, and change the device settings according to the instructions.

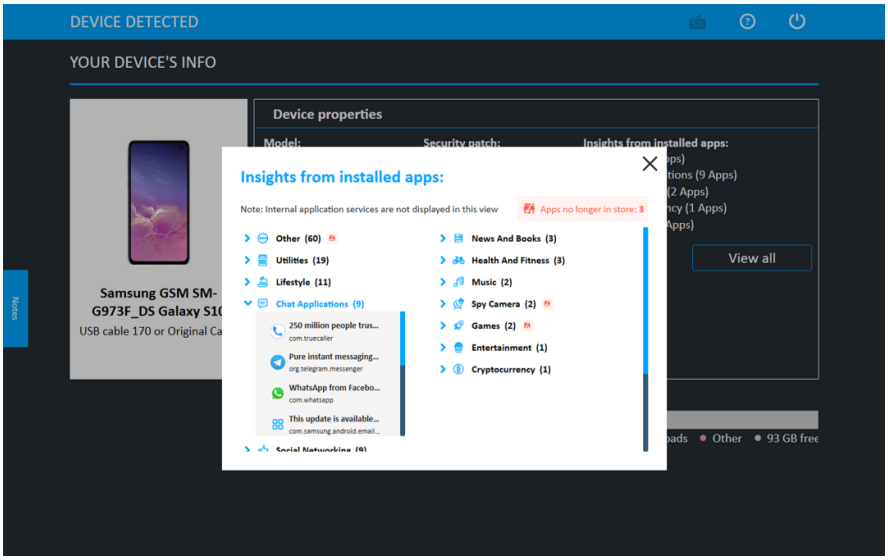
3. Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.
4. Tap **Continue**. The following window appears if the Enable device preview info screen option is enabled under General settings.



This window provides information on the device data before performing an Android extraction. It includes device properties such as model, device name, OS, chipset, whether the device is rooted, date security patch installed, IMEA, the number of installed apps, and insights from installed apps.

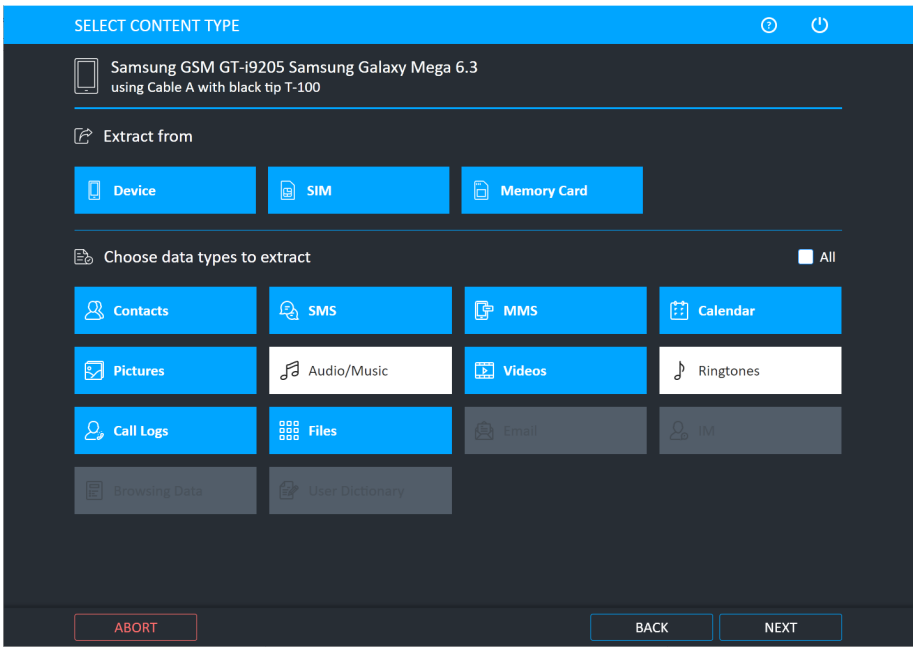
Insights from installed apps allows the user to get a peek into the types of apps installed on the device before the extraction. This areas displays app categories and the number of apps in each. Click View all to view all app insights by category.

To update the app categorization database, go to System settings.



On many devices, but not all, it also includes information on storage volume, data types, volume of storage per data type, and free data.

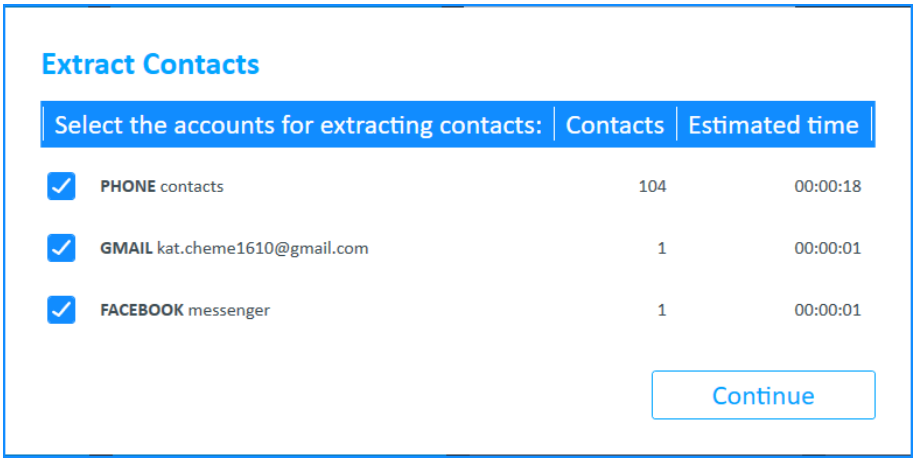
5. Tap **Continue**. The following window appears.



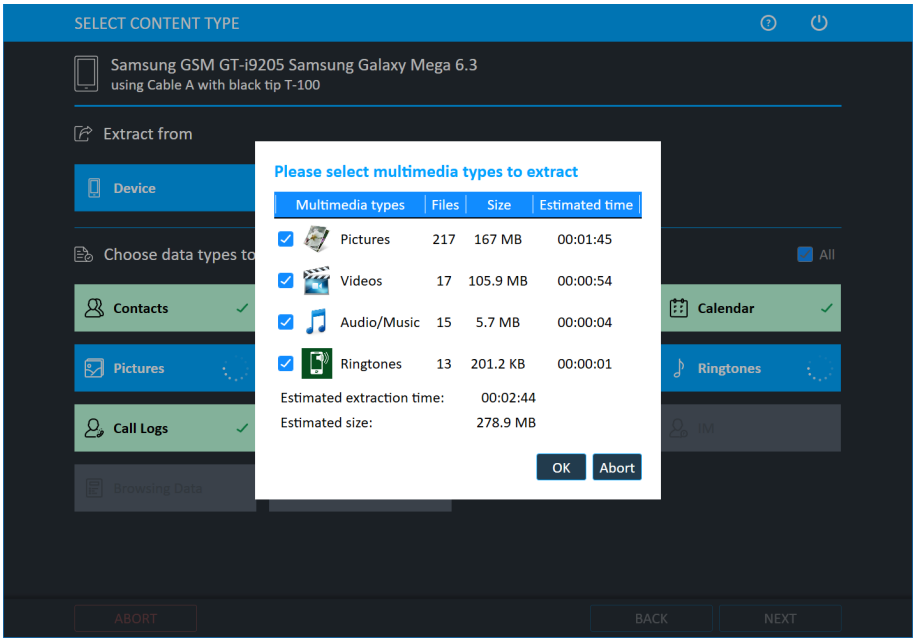
6. Data can be extracted from the Device, SIM and Memory Card of the device. Select from which memory you want to extract.
7. Different data types can be extracted. Select which data types you want to extract. In the example above, music and ringtones are excluded and will not be extracted.

> When Files is selected, UFED performs ADB backup to enable user data to be extracted.

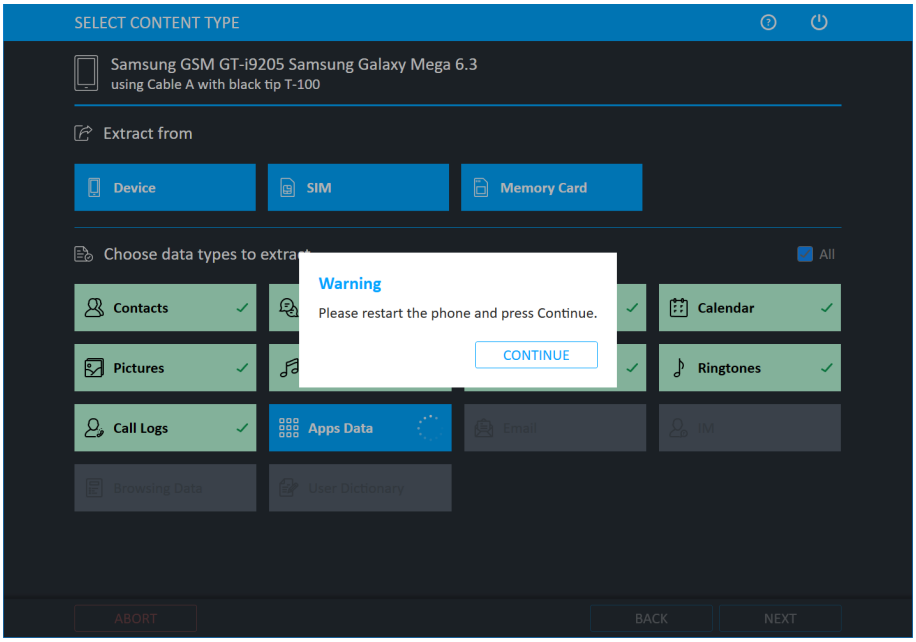
8. Tap **Next**. The following window appears.



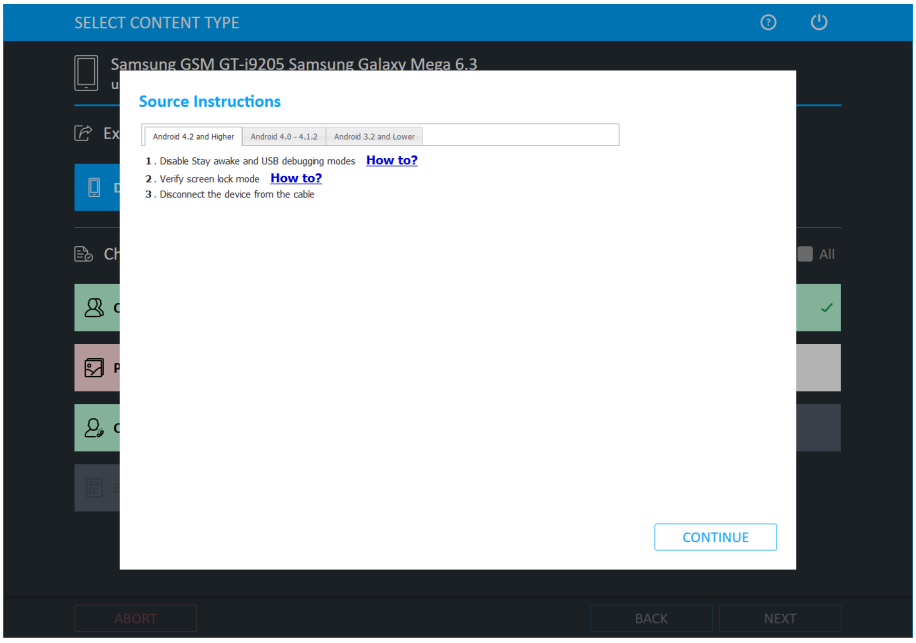
9. Select the required contacts to extract and tap **Continue**. The extraction process starts.



10. Tap **OK**. The following window appears.



11. If required, restart the device then tap **Continue**. When the extraction is complete and if required, the Source Instructions window appears (this depends on the device model). The following window appears.



12. Follow the instructions to return the mobile device settings to the original settings, and then tap **Continue**.

    When the extraction completes, you can perform additional extractions in the Select Extraction Type window or tap **Finish** to create the Extraction Summary. For more information on the Extraction Summary, see Extraction Summary and report data (on page 58).

4. Reporting

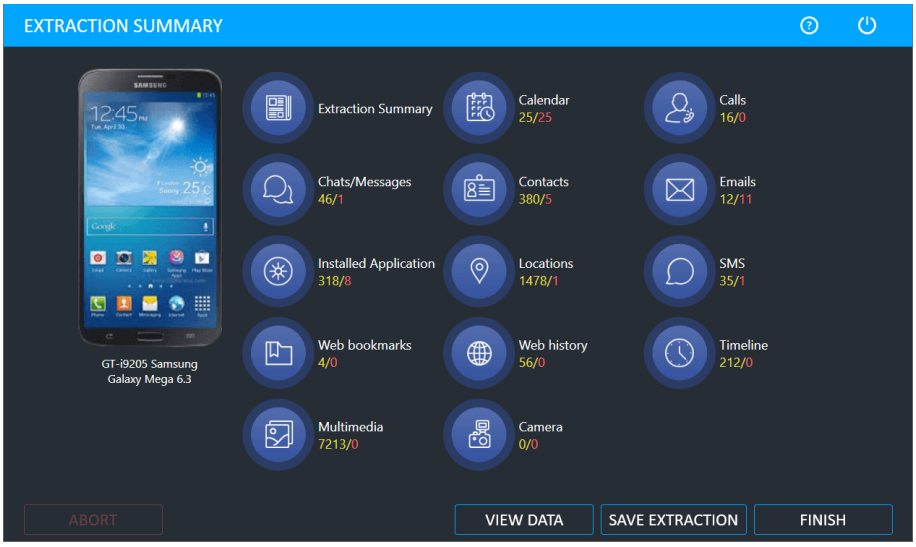
Reporting includes the following sections:

4.1. Extraction Summary and report data

Preview the data, create a report and analyze the data that was extracted.

To view the Extraction Summary:

1. After completing an extraction, the tap **Finish** in the Select Extraction Type window. The Extraction Summary window appears.

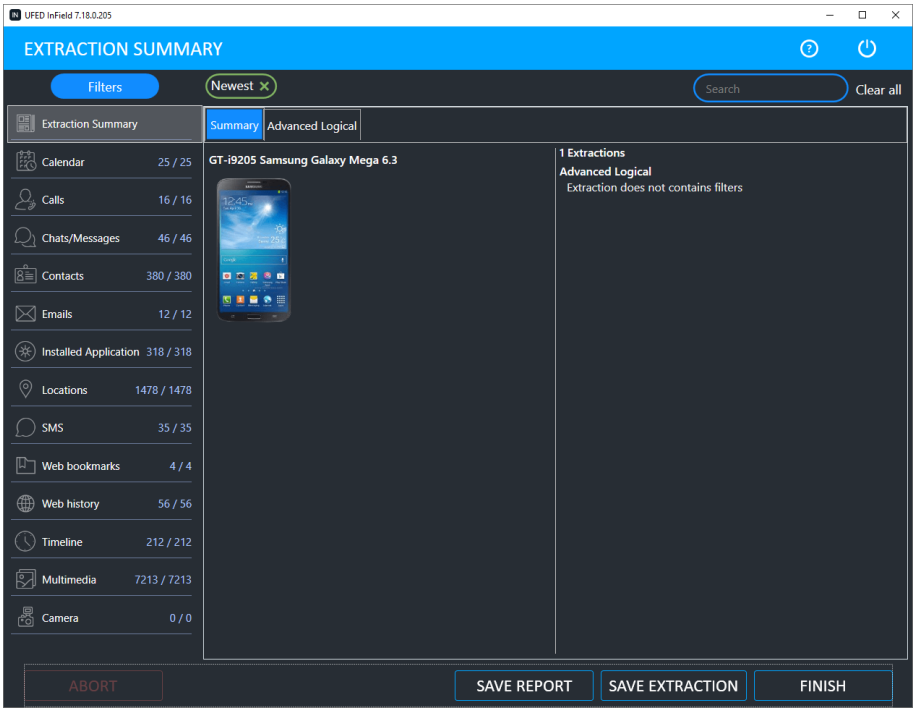


> It takes time to create the Extraction Summary depending on the size of the data extracted .

This window displays a summary of the extracted data. Tap a button to go to a particular section of the report. The numbers in Yellow show the total number of items extracted for each data type. The numbers in Red show the number of items located in deleted data.

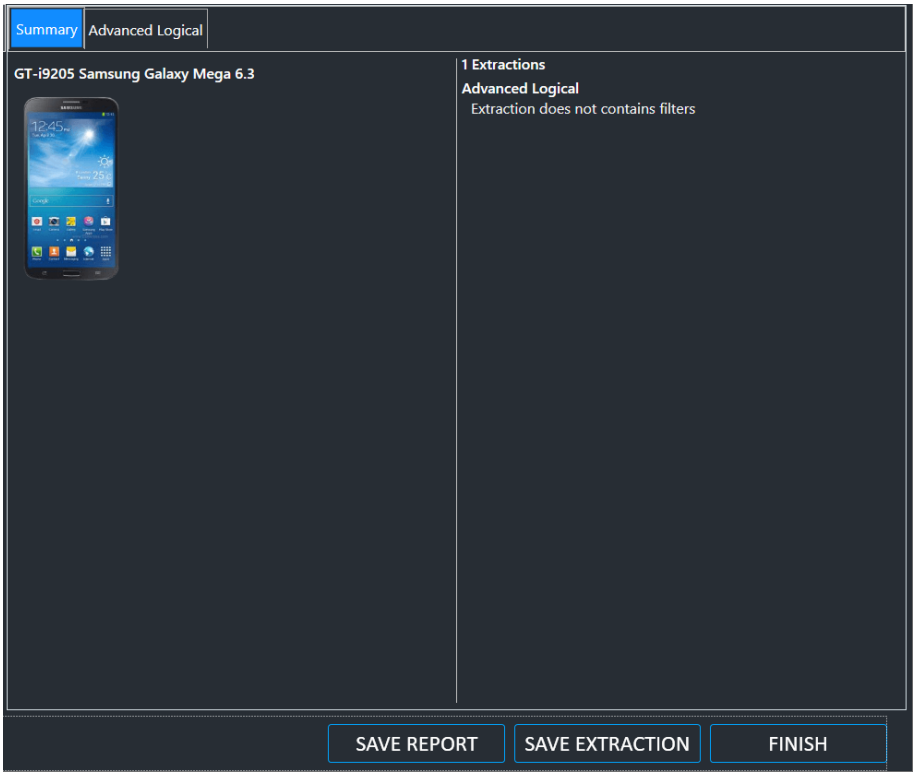
To view the report data:

1. Tap **View data**. The following window appears.

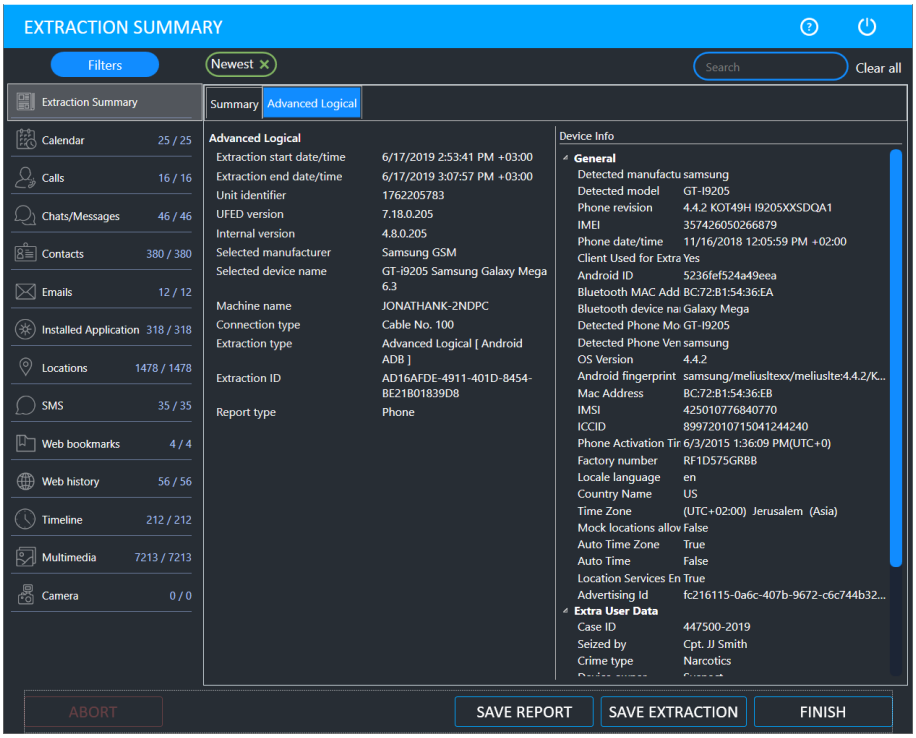


This window enables you analyze the extracted data. You can select filters and data types. Use the search box to search for information.

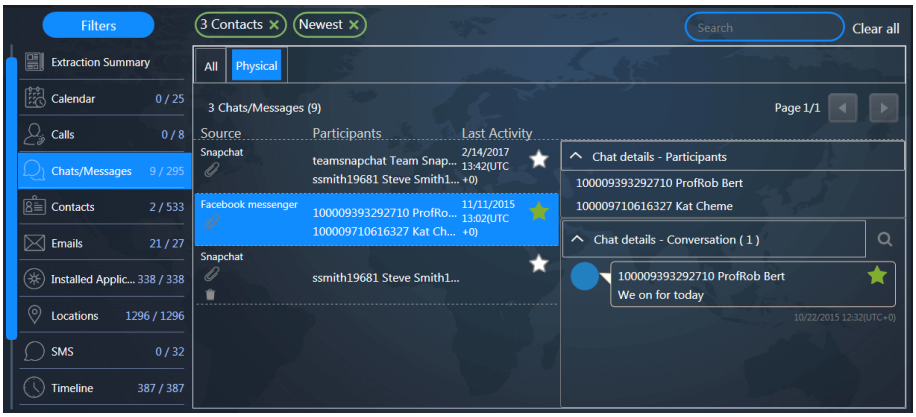
2. Select filters to access more specific data. For more information on filters, see Filtering the data (on page 62).
3. A Summary tab displays case details and information about the extractions (e.g., that the extraction contains all information and filters were not used).



An extraction tab is displayed for each type of extraction performed e.g., Logical, Physical, SMS etc. It includes information such as when the extraction was performed, by what UFED unit, the version number of the unit, extraction ID, unit identifier etc. Device information is also available, such as manufacturer, model, IMEI etc.



4. Select a data type that you want to examine. Data types include Calendars, Calls, Chats, Emails, Installed Apps, Locations, SMS, Timelines, Phone, and Camera (any pictures you took of the device) etc. The following example shows a Chat/Messages data type, with one item bookmarked:



Deleted items are indicated by .

5. Tap **Save report** to save the report (see Saving a report (on page 71)), tap **Save extraction** to save the extraction (see Saving an extraction (on page 74)) and tap **Finish** to close the case (all unsaved data will be lost).

4.2. Report viewer

The Report viewer enables you to open reports, perform your own search and analysis on the analyzed information, and apply filters, generate reports and create bookmarks. The viewer reads UFD (*.ufdx, *.ufd), UFDR (*.ufdr) and zipped UFDR files, which are the report files generated from the analyzed data.

To use the report viewer:

1. From the Home screen, tap **Report**.
2. Navigate to the required file.
3. Tap **Open**. The following window appears.

4. Tap the **Extraction Summary** button to view the Extraction Summary.
5. Tap **View data** to display a report of the data (see Extraction Summary and report data (on page 58)), tap **Save extraction** to save the extraction (see Saving an extraction (on page 74)) or tap **Finish** to close the case (all unsaved data will be lost).

4.3. Filtering the data

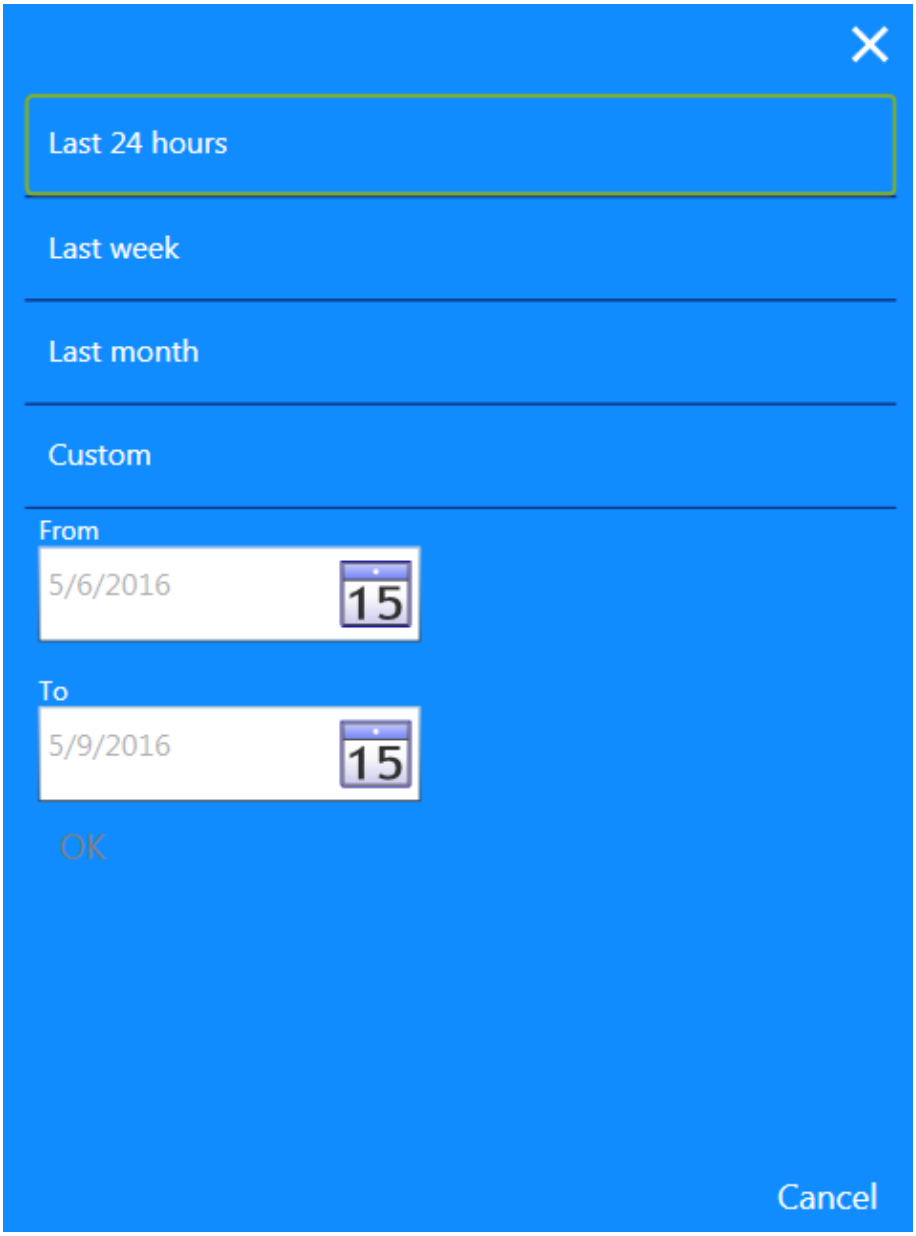
Analyze data using simple data filters such as timelines, contacts, crime-related watch lists, bookmarks, and sort order. The left section of the reporting window contains options for filtering the extracted data. Use the filters to drill-down to the granular data. Use the following filters to narrow down the displayed data:

- Filtering by time (on the facing page)
- Filtering by contacts (on page 66)
- Filtering by watch lists (on page 68)
- Filtering by bookmarks (on page 69)
- Filtering by sorting (on page 70)

To clear all the selected filters, tap **Clear**.

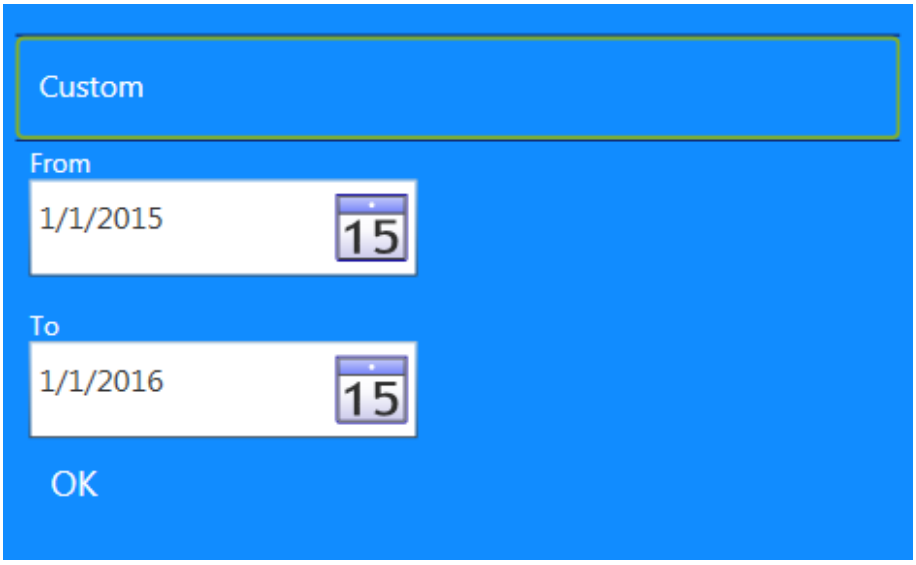
4.3.1. Filtering by time

Filter data based on date and time using pre-defined filters such as: Last 24 hours, Last week, Last month, or custom.



To create a custom timeframe:

1. Tap **Custom**.

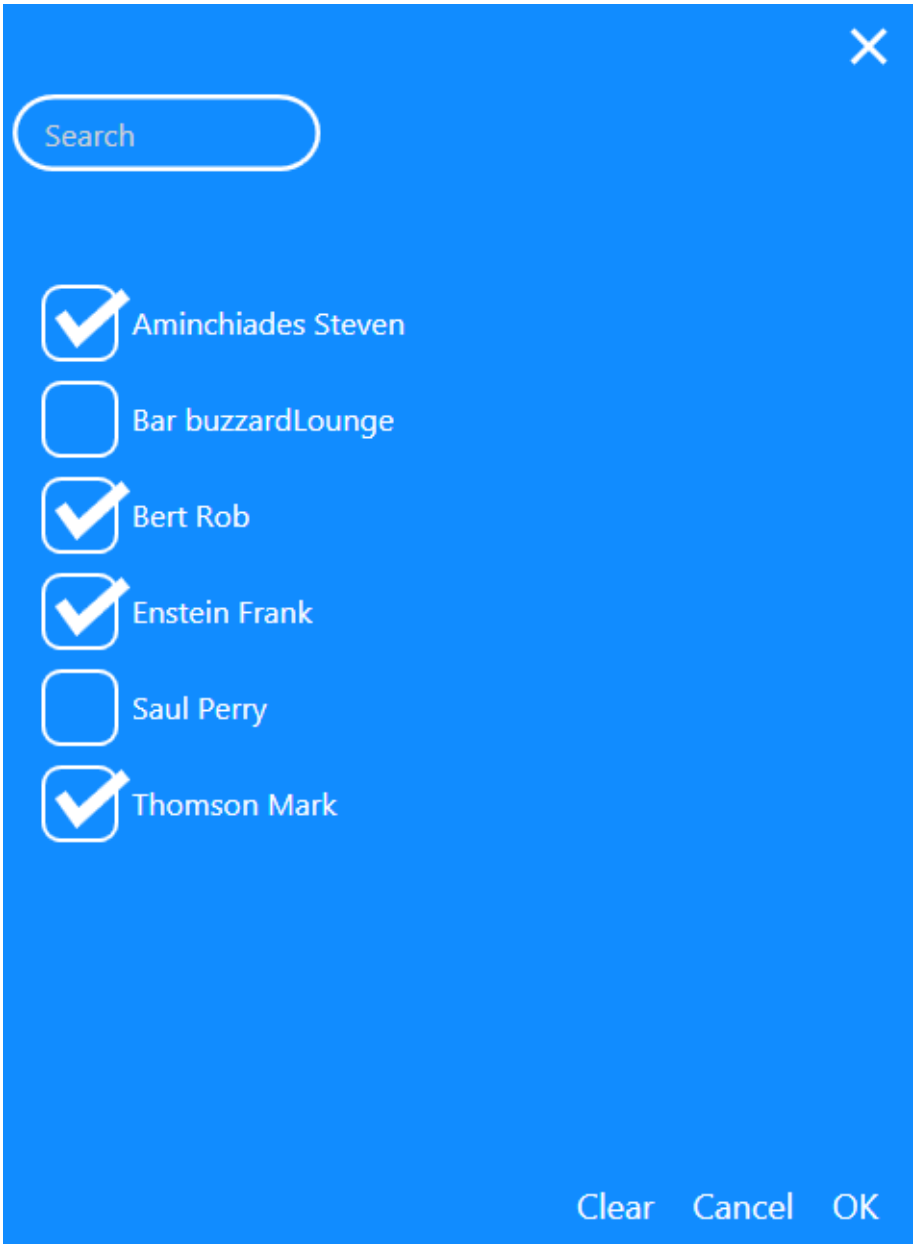


2. In the From and To boxes, enter the date or tap 15, and select the date from the calendar.
3. Tap OK to create the custom filter.

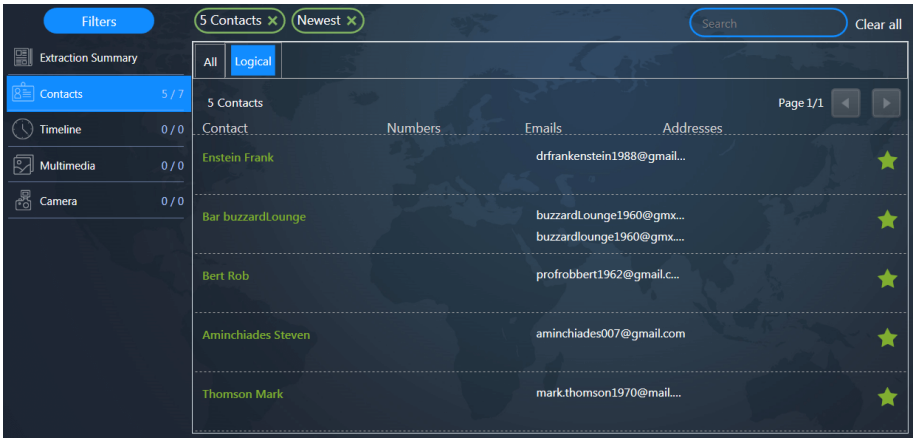
4.3.2. Filtering by contacts

To select the contacts that you want to analyze:

1. Tap the Contacts filter. The following window appears.



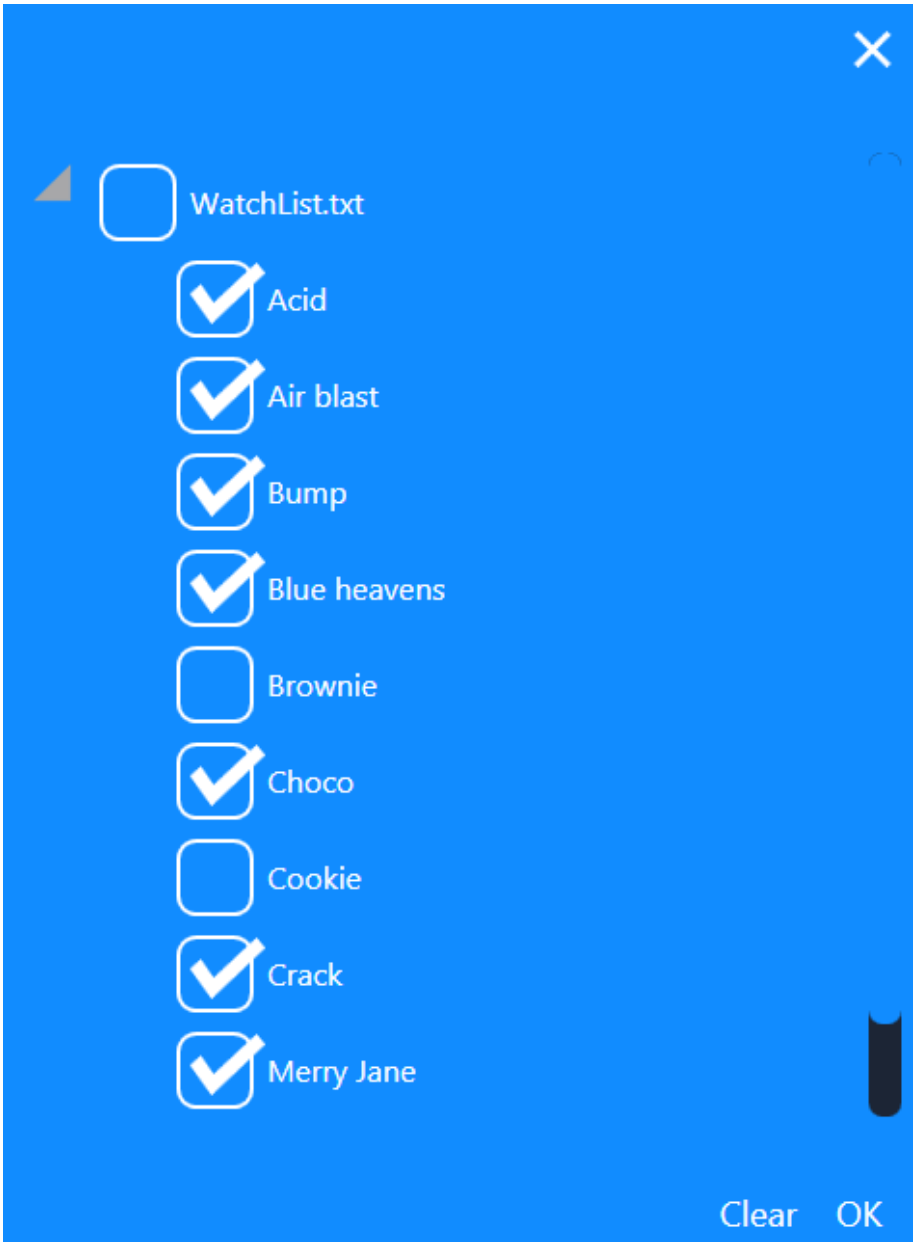
2. Select the required contacts and tap OK. The selected contacts are displayed under the Contacts filter.



3. To edit the list of contacts, tap **Filters** > **Contacts**.

4.3.3. Filtering by watch lists

A watch list is a list of key words that can be used to identify and highlight important and relevant information. An XML watch list, needs to be imported into Cellebrite Responder before it can be used. If a new watch list is uploaded it will replace the existing watch list. Each imported watch list can include a maximum of 100 key words per crime type. For information on importing a watch list, see Importing settings and configuration files (on page 109).



4.3.4. Filtering by bookmarks

A bookmark is a quick reference pointer for individual items.

To create, display and clear bookmarks:

1. Tap ☆. The selected bookmark changes to ★.
2. To display only the bookmarked data, select Bookmarks in the Bookmark filter.

4.3.5. Filtering by sorting

Select the order in which you want the displayed data to be sorted. Newest data first (Newest) or the oldest data first (Oldest).

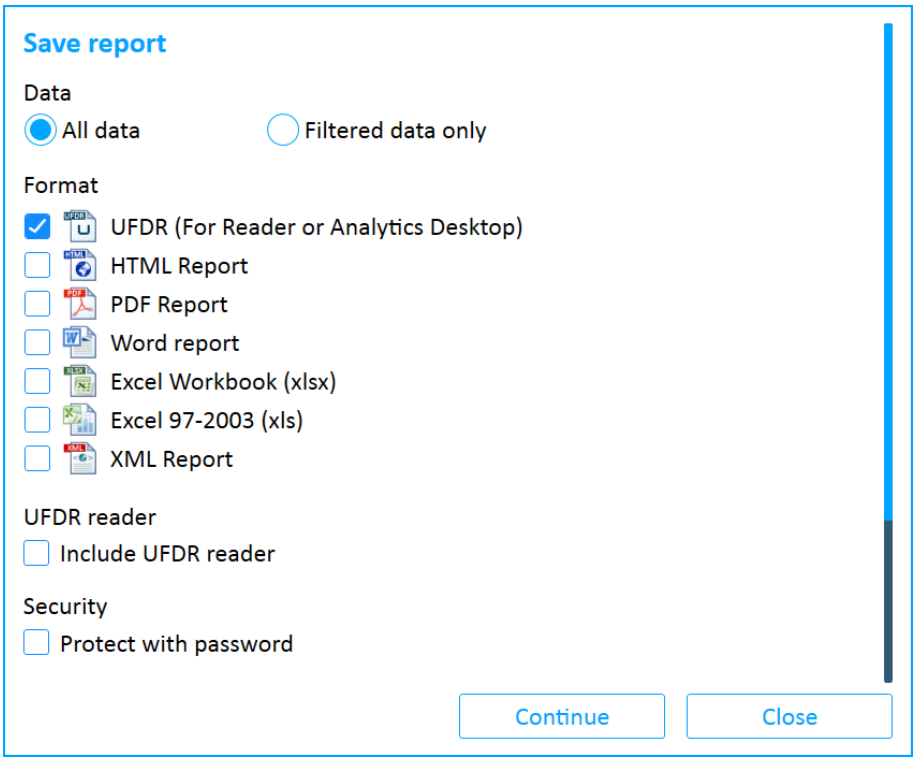
4.4. Saving a report

When saving a report, you can select the following options:

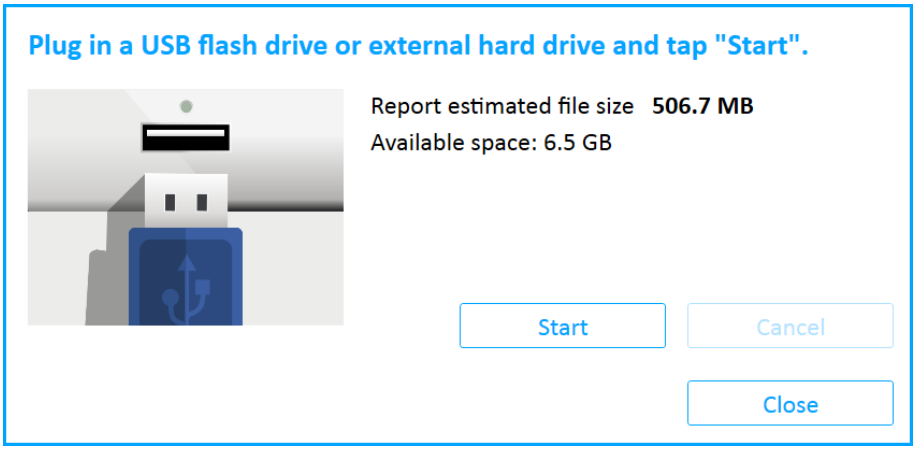
- **Data:** All the data or only the filtered data.
- **Format:** HTML, PDF, Word, Excel Workbook, Excel 97-2003, XML and UFDR (for the Reader, or Pathfinder Desktop) formats.
- **Security:** Protect the report with a password. The password must be a minimum of 8 and a maximum 10 alphanumeric characters.
- **Destination:** You can save the report to a USB device, Network (if defined under **Settings** > **Storage**), Disc (different types supported), or Local Drive (not applicable to kiosk's).

To save a report:

1. Tap **Save Report**. The following window appears.



2. Select the required options and then tap **Continue**. The following window appears.



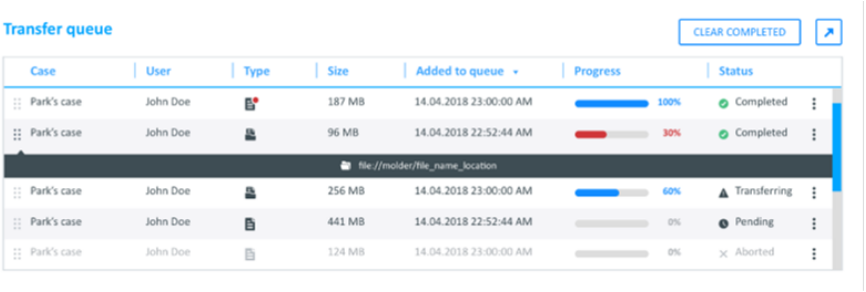
The system indicates the number of discs required for the selected disk type. You will also be notified to insert the new disks, if required.

3. Tap **Start**.

Managing network file transfers:

When saving reports to a network drive, it is possible to continue working in Cellebrite Responder during the file transfer process. All transfer file details can be viewed in the Transfer queue.

1. To open the Transfer queue, click  at the top of the screen.



2. View Transfer details including case, user, type, size, time added to queue, progress, and status. Users can see only their transfers, admins can see all file transfers.
3. If necessary, click on the menu icon in a transfer row to take one of the following actions:
   - Retry
   - Remove from list
   - Change target location
   - Abort transfer

To clear all completed transfers, click CLEAR COMPLETED.

To minimize the Transfer queue window, click .

4.4.1. Viewing the saved report

The extracted data is saved in the location you selected. The extracted data folder contains:

- Multimedia files folders named Audio, Icons, Images, Ringtones, and Video folders, containing each of the respective type of media files.
- Snapshots with any images that you captured.
- Resource files such as pictures in the HTML file.
- HTML, PDF, Word, Excel, XML, and UFDR (for the Reader or Pathfinder Desktop) files.

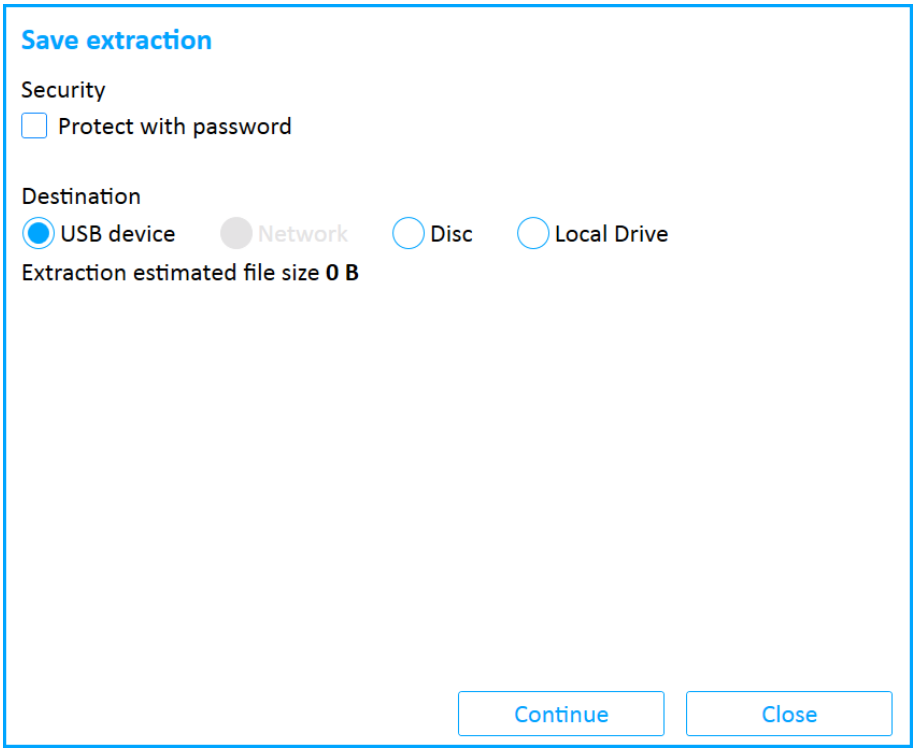
4.5. Saving an extraction

When saving an extraction, you can select the following options:

- **Security:** Protect the extraction with a password. The password must be a minimum of 8 and a maximum 10 alphanumeric characters.
- **Destination:** You can save the extraction to a USB device, Network (if defined under **Settings** > **Storage**), Disc (different types supported), or Local Drive (not applicable to kiosk's).

To save an extraction:

1. Tap **Save extraction**. The following window appears.



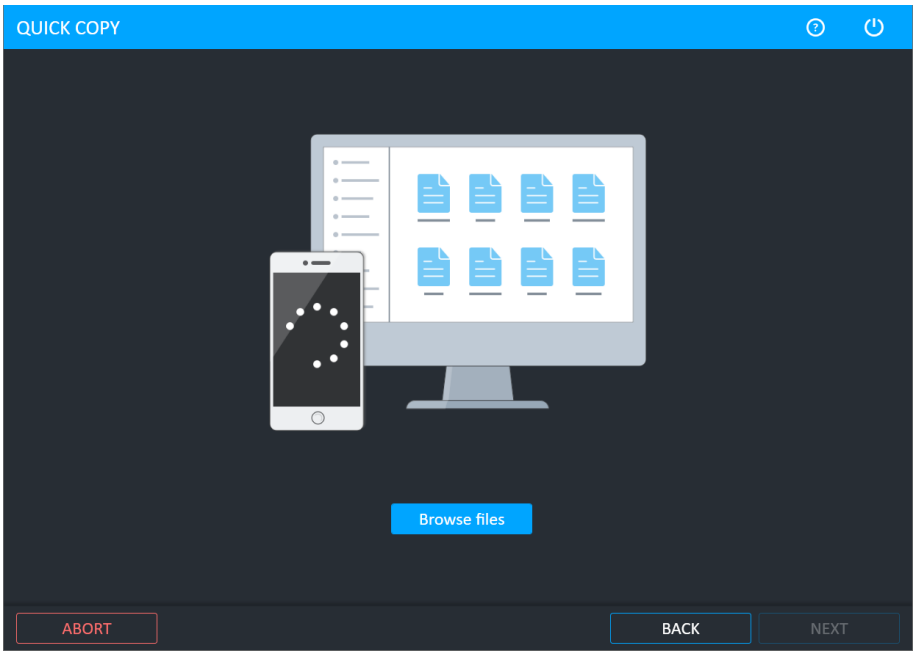
2. Select the required options, tap **Continue** and follow the on-screen instructions.

5. Quick copy

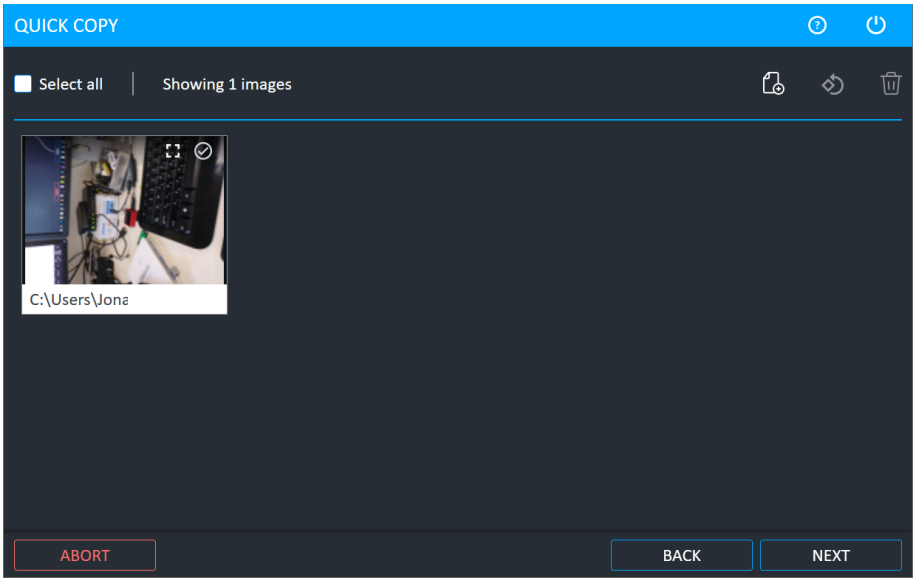
Quick copy provides the ability for witnesses and victims to share specific evidence with law enforcement agencies in an unobtrusive manner, without affecting their mobile device. This feature can be used to connect to a device quickly, using a cable, and to copy a specific file or picture from the device.

To use quick copy:

1. From the Home screen, tap **Quick copy**.
2. Enter the case details and tap **Continue**. The following window appears.



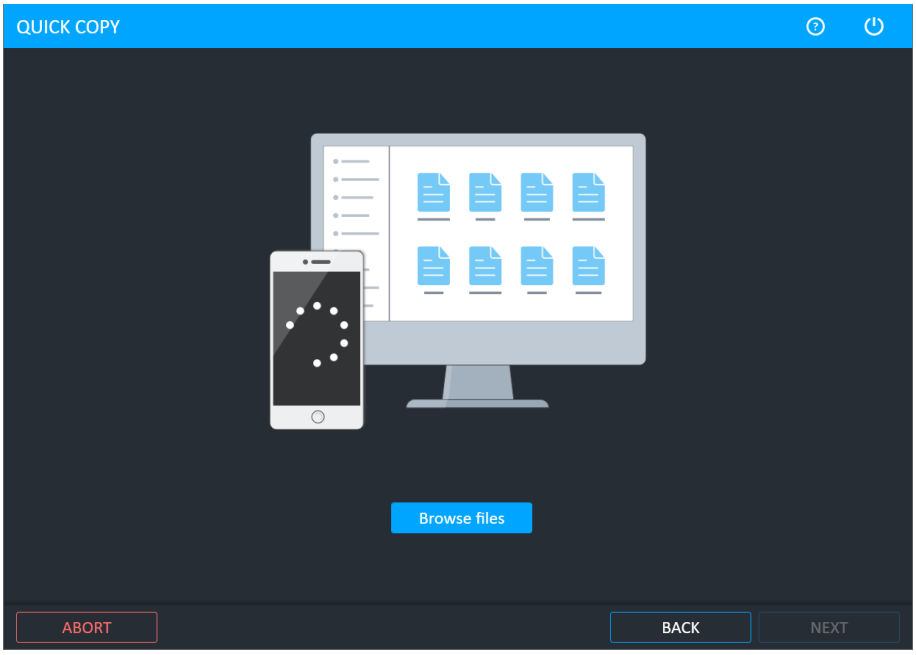
3. Make sure that the device is connected to a USB port, then tap **Browse files** to navigate to the device, select the files that you would like to copy and then tap **Open**. The following window appears.



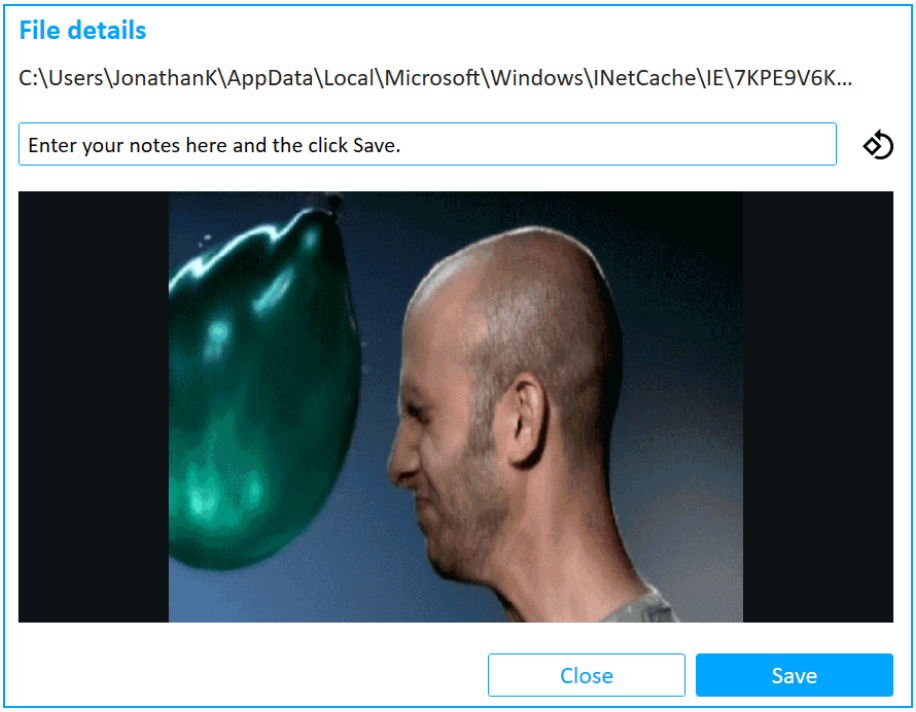
4. Tap add ( ) to an additional file.

5. Tap rotate ( ) to rotate images and videos.

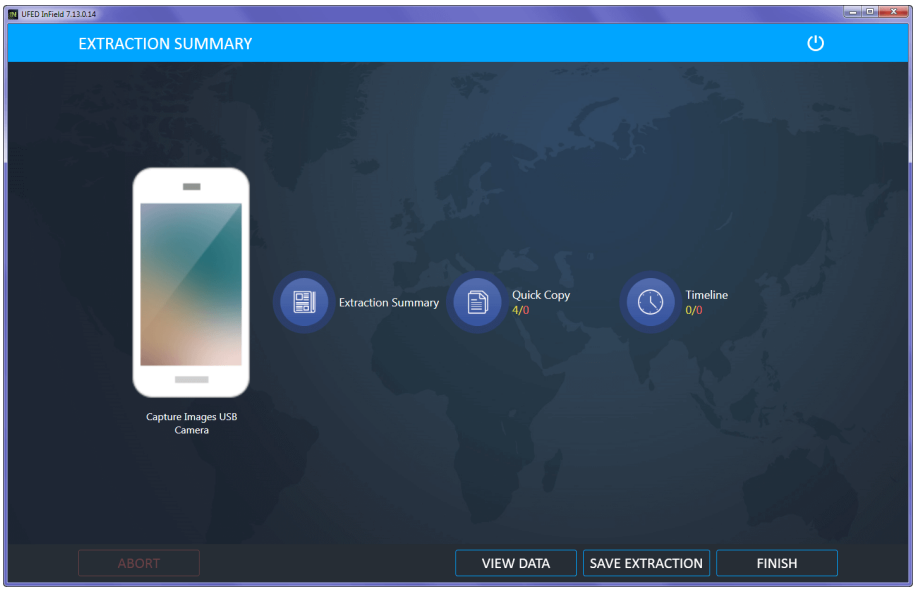
6. Tap delete ( ) to delete a file.



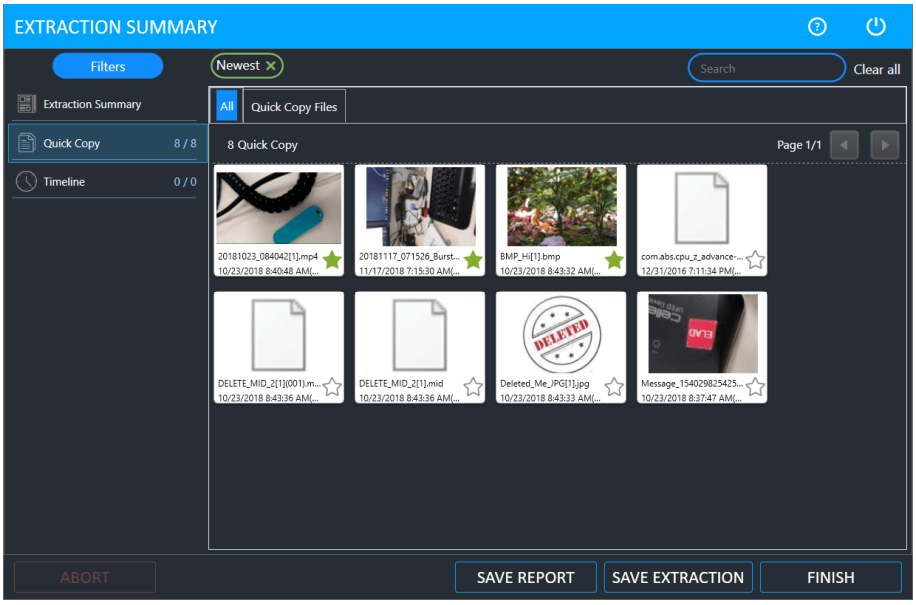
7. If required, you can add notes to each file.



8. Select the **Select all** check box to select all files. Tap the check mark to include ( ) or exclude ( ) files.
9. Tap **Next** to copy the files. The following window appears.



10. Tap **Extraction Summary** or **Quick Copy** to display the items in the Extraction Summary. The copied items can be viewed under Quick Copy.



11. Tap **Save report** to display a report of the data (for more information see Extraction Summary and report data (on page 58)), tap **Save extraction** (see Saving an extraction (on page 74)) or tap **Finish** to close the case (all unsaved data will be lost).

6. Settings

The settings screen provides access to a set of functional and behavioral setup options used to control the functionality and usability of Cellebrite Responder.

To access the settings screen, tap the menu icon in the application taskbar and select Settings..

The settings are grouped in the settings screen in the following tabs:

The settings screen opens on the **General** tab.

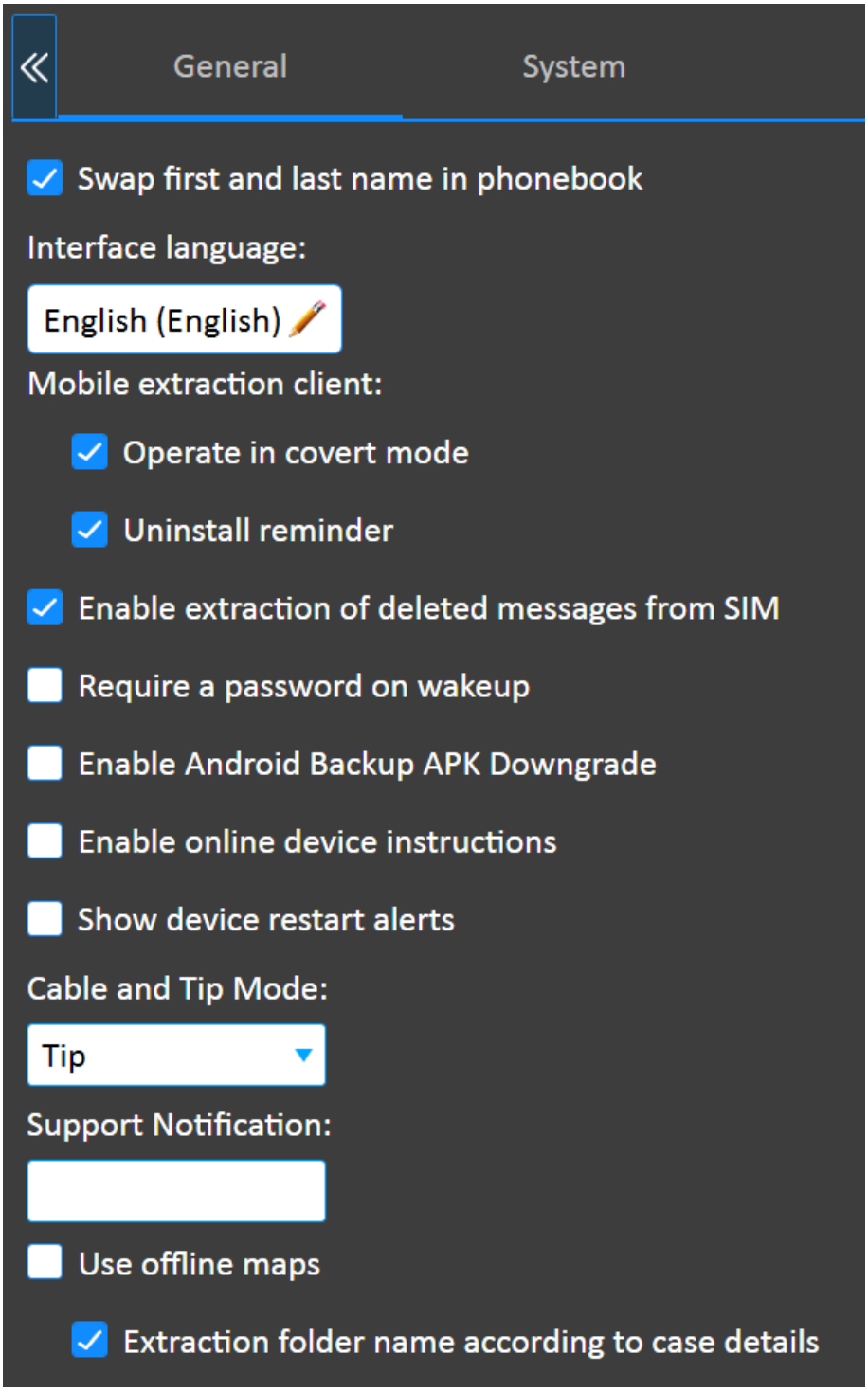
When using the Cellebrite Commander, some or all of these settings may be managed by Cellebrite Commander.

Changes that are made to the settings via Cellebrite Commander or manually by a user, will affect all users on the same machine.

6.1. General settings

The settings window opens on the **General** tab.

Some general settings can also be set using Cellebrite Commander. For more information, refer to the Cellebrite Commander manual.



The **General** tab provides access to the following functions and settings:

Setting	Description	Default
Swap first and last name in phonebook	Swaps the first and last name in phone book entries.	Selected
Interface language	Changes the interface language. For more information, see Changing the application interface language (on page 85)	English
Operate in covert mode	Renames the application client name from "Cellebrite.sis/exe" to "AAA.sis/exe".	Selected
Uninstall reminder	When enabled, the Cellebrite Responder prompts you to uninstall the client from the examined device.	Selected
Enable extraction of deleted messages from SIM	Extracts deleted messages from a SIM. This check box is selected by default.	Selected
Enable Android Backup APK Downgrade	Enables the Android Backup APK Downgrade method. This check box is selected by default.	Selected

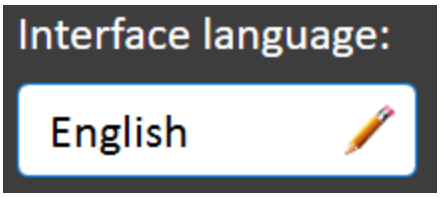
Setting	Description	Default
Enable online device instructions	Displays the online device instructions instead of the offline device instructions. This check box is not enabled by default. This setting is for the Waiting for Device instructions, which explains how to connect a source device to UFED. If you have network performance issues when using the online device instructions, clear this check box.	Not selected
Show device restart alerts	Displays device restart alerts during the extraction process. This check box is selected by default.	Selected
Cable and Tip mode	Indicates the cable or tip to be used during the extraction.	Tip
Support Notification	Enter a text message that will be displayed to Cellebrite Responder users at the bottom of the screen. For example, "Contact the admin at ext 224 if you have any questions".	
Use offline maps	Uses offline maps when selected.	Not selected

Setting	Description	Default
Show investigation notes	Displays the Investigation notes widget, which enables you to add pictures, screen shots and text to document the investigation. See Investigation notes (on page 37).	
Disc catalog ID	Select **Disc catalog ID**. When this check box is enabled, you can enter a disk catalog ID when burning extractions and reports to discs.	
Examination tool	Use Cellebrite Responder viewer or Physical Analyzer as the examination tool to view the decoded data. Changing the examination tool, from the default Cellebrite Responder viewer, is only possible if Physical Analyzer and Cellebrite Responder are installed on the same computer.	
Choose additional logo	Select an additional logo that will be displayed in the title bar of the home screen. Now when an extraction completes instead of the View data button the Open in Physical Analyzer button will be displayed in the Extraction Summary window.	
Save report automatically	Select to automatically save the extraction report.	

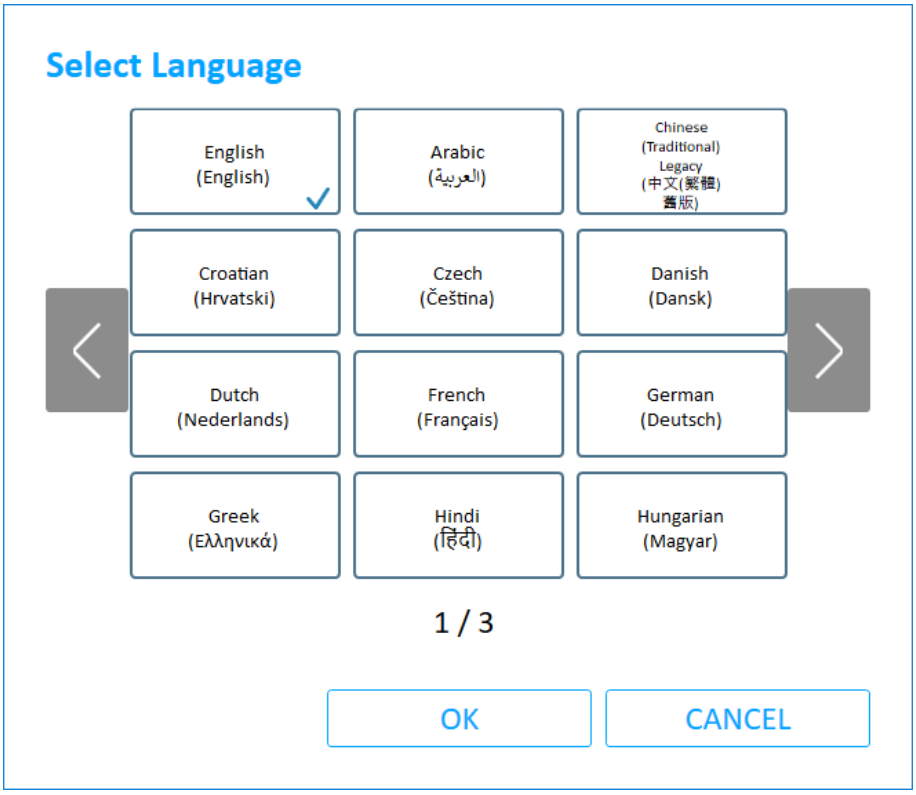
Setting	Description	Default
Video quality	Set the video quality of the UFED camera to Best (1920 x 1280), Normal (1024 x 1280 default) or Low (640 x 480).	Normal
Enable device info (Advanced logical)	Displays the Device Info window during the Advanced Logical extraction. This window provides information on the device data, before performing an Android extraction.	Selected

6.1.1. Changing the application interface language

1. Tap the language field.

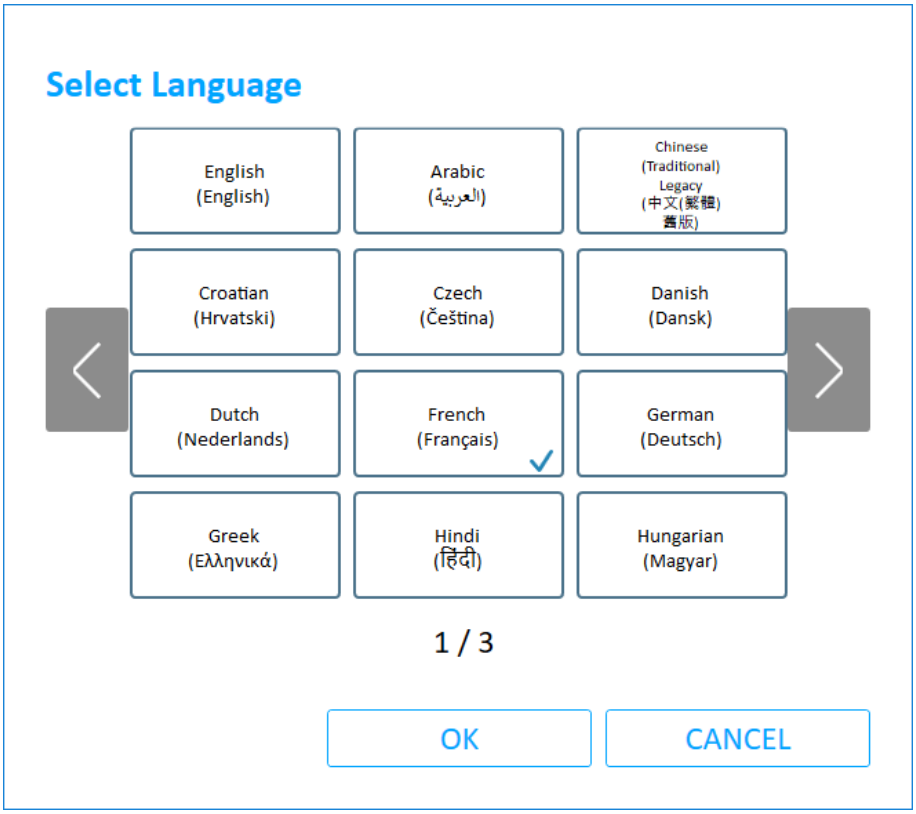


The Select Language screen appears with the current language selected. (In this case, English).

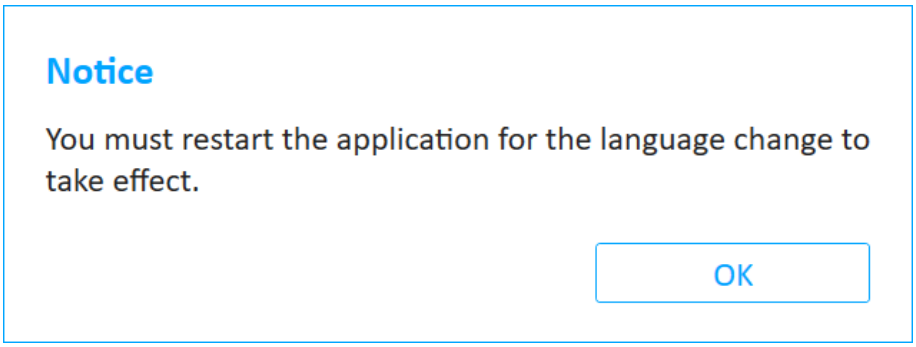


Use the arrows to scroll through the list of available interface languages.

2. Tap the required language.



The following message appears (in the selected language):



3. Tap **OK**.

   The **General** tab appears with the language of choice in the Interface language field.

4. Tap **Save** to close the Settings panel.
5. To restart the application:

   a. To close the application, tap  in the application taskbar.

   b. To restart the application, do one of the following:

      - Tap the application shortcut icon located in the UFED shortcuts panel at the right of the screen.
      - Double-tap the **Cellebrite Responder** icon located on the Desktop.

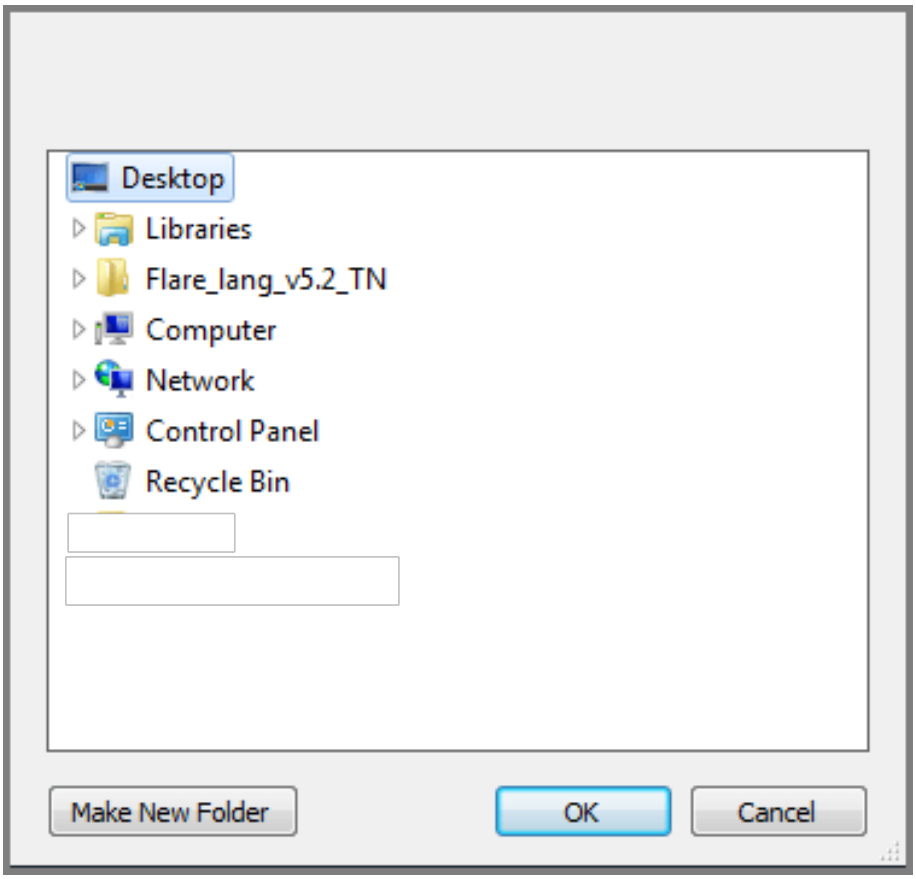
- Tap **Start** > **Cellebrite Responder**
- Tap **Start** > **All Programs** > **Cellebrite Mobile Synchronization** > **Cellebrite Responder**.

Cellebrite Responder starts in the selected language.

If Simplified Chinese is added to the Cellebrite UFED license, you will need to restart the application before the change will take effect.

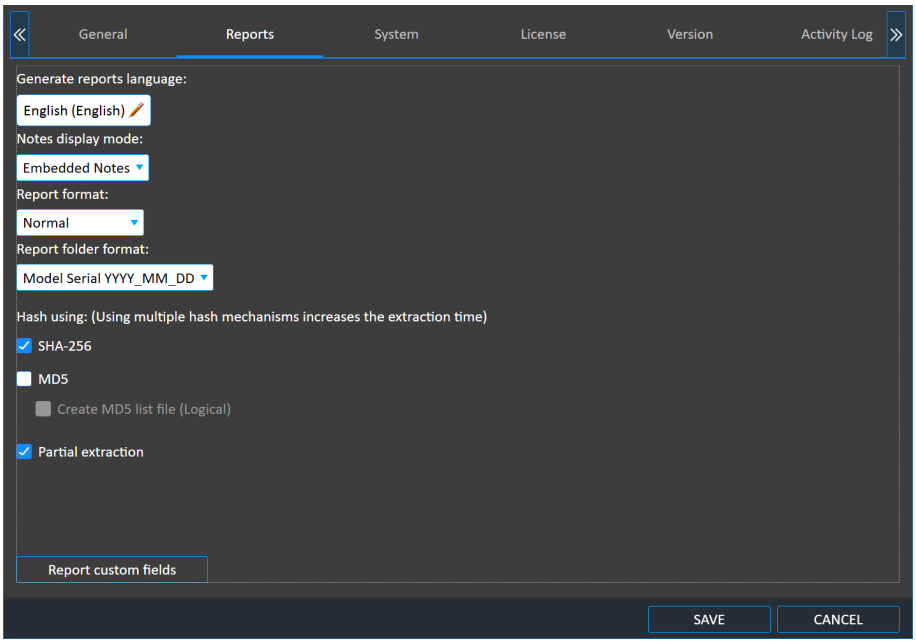
6.1.2. Changing the extraction location

1. In the **Save extractions to** area, click **Browse**. The Browse for folder dialog appears.



2. Select the folder where you want to save the extraction files, and click OK.

6.2. Report settings



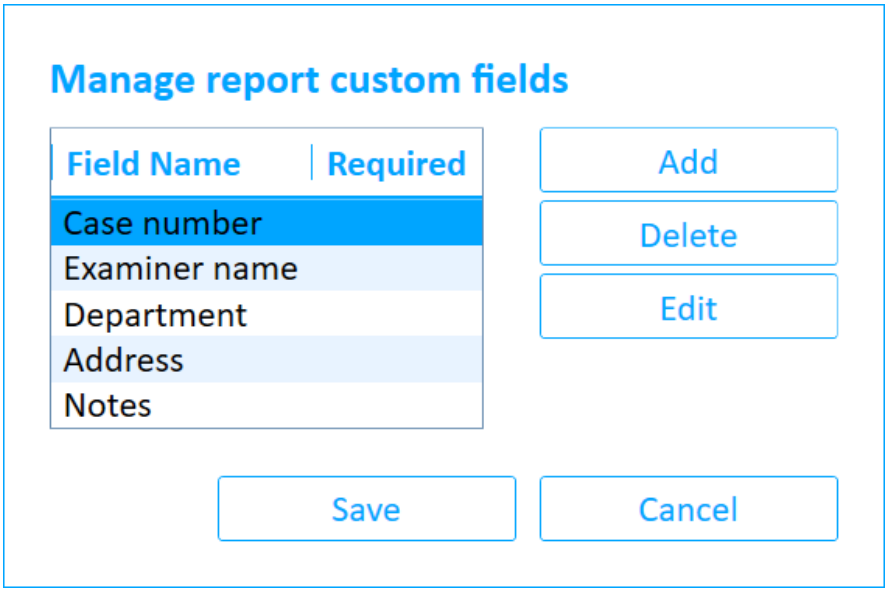
To set the report settings:

1. Access the **Settings** > **Reports** tab.
2. To set the generated reports language, tap  next to **Generate Reports Language**, and select the desired language.
3. To set how the known issues notes about the extracted device are logged in the generated report, tap  next to **Note display modes**, and select one of the following:
   - **Disable** – Do not include device specific notes in the report.
   - **Separated Notes** – Add all the device specific notes at the end of the report.
   - **Embedded Notes** – Device-specific notes follow the content type they refer to in the report.
4. To set the generated reports visual formats, tap  next to **Report format**, and select one of the following:
   - **Normal** – The standard report structure, suitable to standard display screens.
   - **Compact** – A compact report structure, suitable for devices with a small display area.

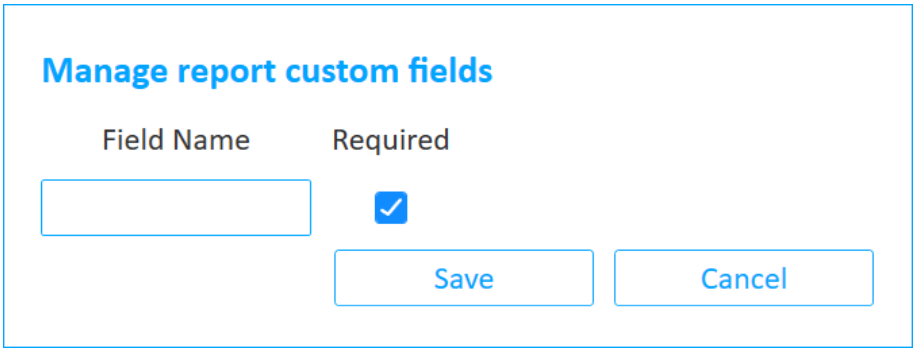
5. To set the generated reports folder name formats, select  next to **Report folder format**, and select one of the following:
   - **Model Serial YYYY_MM_DD** – The folder name is constructed from <the model name> <the model serial> <the year in 4 digits>_<the month in 2 digits>_<the day in 2 digits>
   - **YYYYMMDD Model Serial** – The folder name is constructed from <the year in 4 digits><the month in 2 digits><the day in 2 digits> <the model name> <the model serial>
6. Select or clear **Hash using MD5** to toggle the display of the MD5 values which are generated for each file in the extracted data. This increases the time required to complete the extraction.
7. Select **Create MD5 list file** to generate a Checksums.md5 file that contains all the generated MD5 values of the extracted data.
8. Select or clear **Hash using SHA-256** to toggle the display of the SHA-256 values which are generated for each file in the extracted data.
9. Select or clear **Partial Extraction**, in the event of an extraction error, whether or not to include the partially extracted data up to the error point in the generated report.
10. Tap **Report custom fields** to add, remove and edit report fields. For more information, see Managing report fields (on the facing page).
11. To set a field as required, tap the field in the **Required** column.
12. Tap **Save**.

6.2.1. Managing report fields

1. Tap **Report custom fields** to customize the report by defining additional fields which will be filled at the end of the extraction.



2. To add a new field:
   a. Tap **Add**.



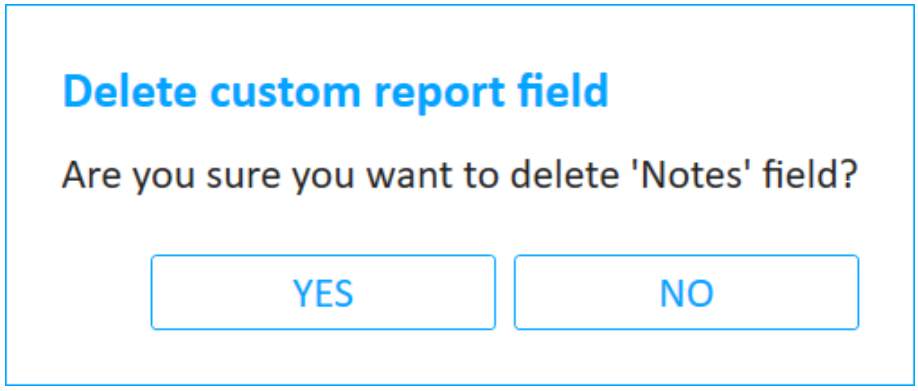
   b. Enter the field name in the **Field Name** box.

> To display the keyboard, tap **Keyboard**.

   c. To set the field as mandatory, select **Required** next to the field name.
   d. Tap **Update**, or to exit without saving, tap **Cancel**.
3. To add additional fields, repeat step 2.
4. To edit an existing field:
   a. Tap the field in the list, and tap **Edit**.
   b. Repeat steps 2b-2d.

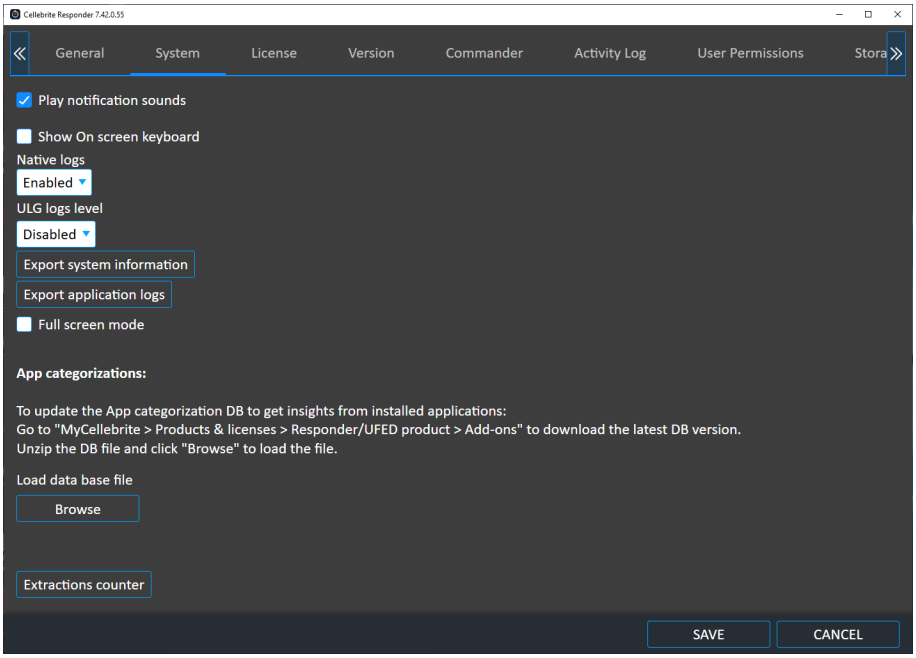
You cannot edit the field name of a default custom field.

5. To delete a field:
   a. Tap the field in the list, and tap **Delete**.



   b. In the confirmation message, tap **Yes**.
6. Tap **Save** in the **Reports** tab.

6.3. System settings



Define the following additional settings in the System tab:

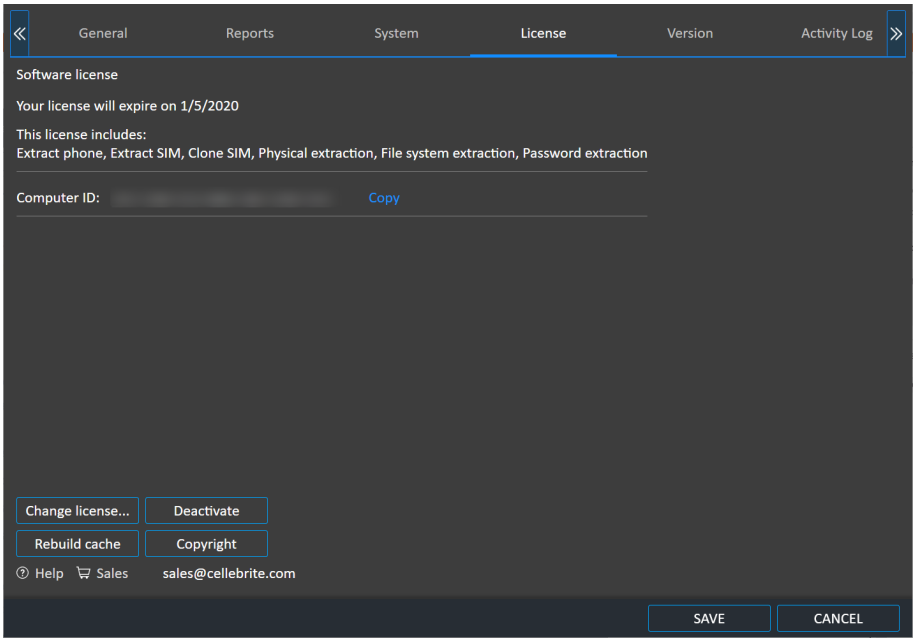
- To set Cellebrite Responder to alert you when your attention is required, such as when it is waiting for your input or when an extraction fails, select **Play notification sounds**.
- To show or hide the on-screen keyboard, select or clear the **Show on screen keyboard** check box. This check box is selected by default.
- To change the **ULG logs level**, select one of the following:
  - **Disabled** – The system will not generate log files.
  - **Detailed** – The system will generate detailed log files. The transaction will be slower in order to write to the log. Recommended in case of debugging/error situation.
- To export system information, tap **Export system information**.
- To save the application logs, tap **Export application logs**.
- To update the App categorization DB to get insights from installed applications, go to **MyCellebrite > Products & licenses > Cellebrite Responder > Add-ons** to download the latest DB version. Unzip the DB file and click Browse to load the file.
- To monitor device usage, tap the **Extractions counter**. This counts the number of extractions performed by Cellebrite Responder. Transactions include all extractions per type and device tool actions. The counters are managed locally and can be reset.

> The password to reset the Extractions counter is the Computer ID or dongle serial number (displayed in the **License** tab).

6.4. License settings

Change the license type in the **License** tab.

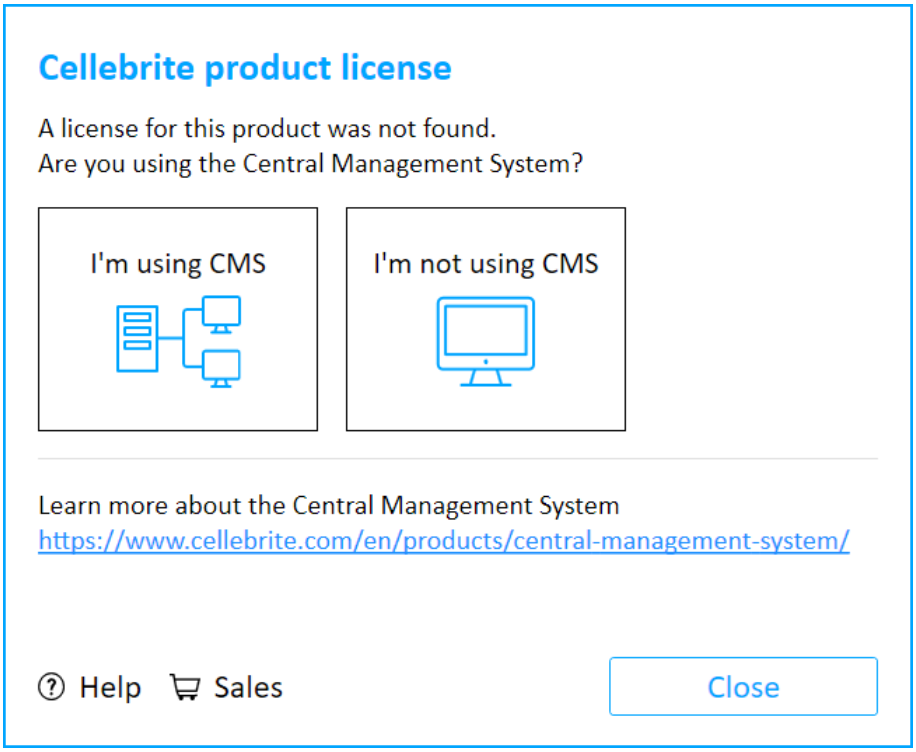
The current license type is displayed.



To change the license type, follow the instructions in Activating the license (on page 24).

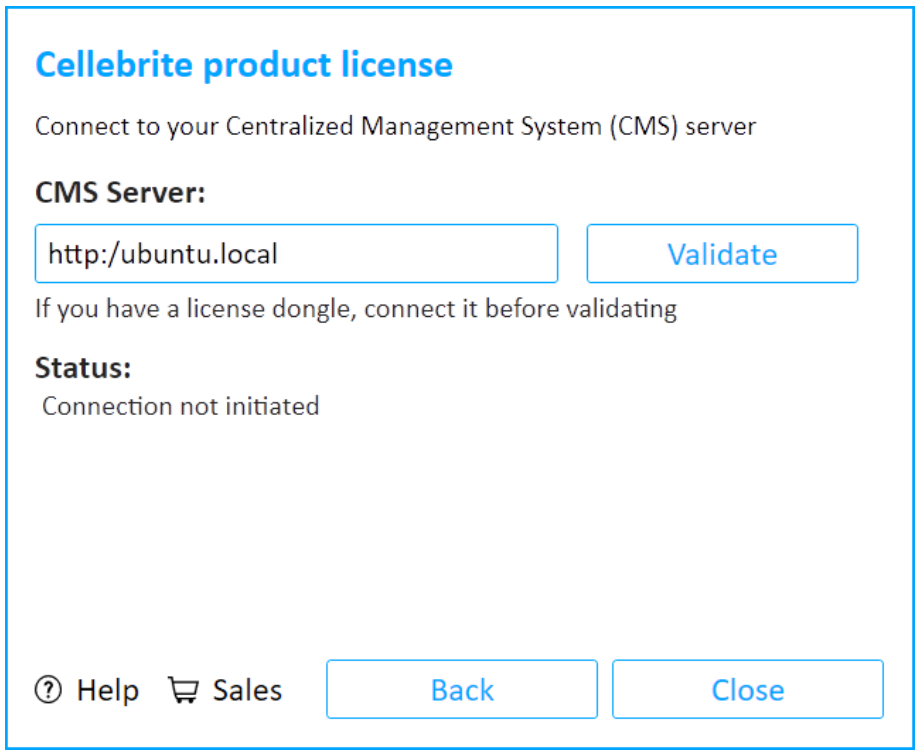
6.4.1. License not found

If a license cannot be found the following window appears.



If you are using Cellebrite Commander:

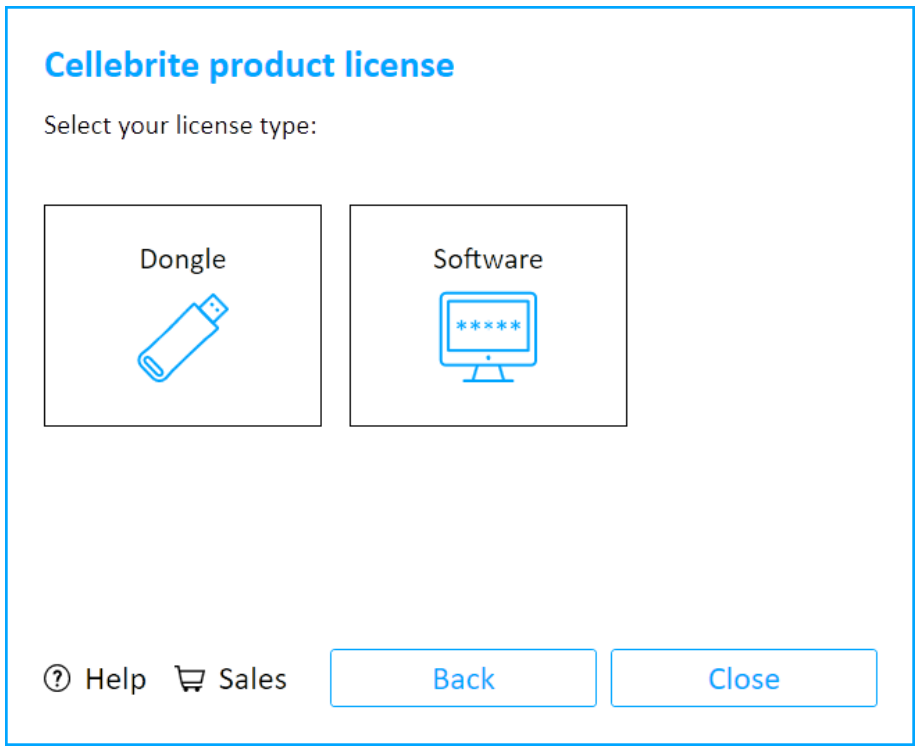
1. Tap **I'm using Cellebrite Commander**. The following window appears.



2. Connect the license dongle before validating.
3. Enter the Cellebrite Commander Server information. For more information on entering the information in this window, see Connect a Cellebrite UFED device to Cellebrite Commander (on page 107).
4. Tap **Validate**.

If you are not using Cellebrite Commander:

1. Tap **I'm not using Cellebrite Commander.** The following window appears.



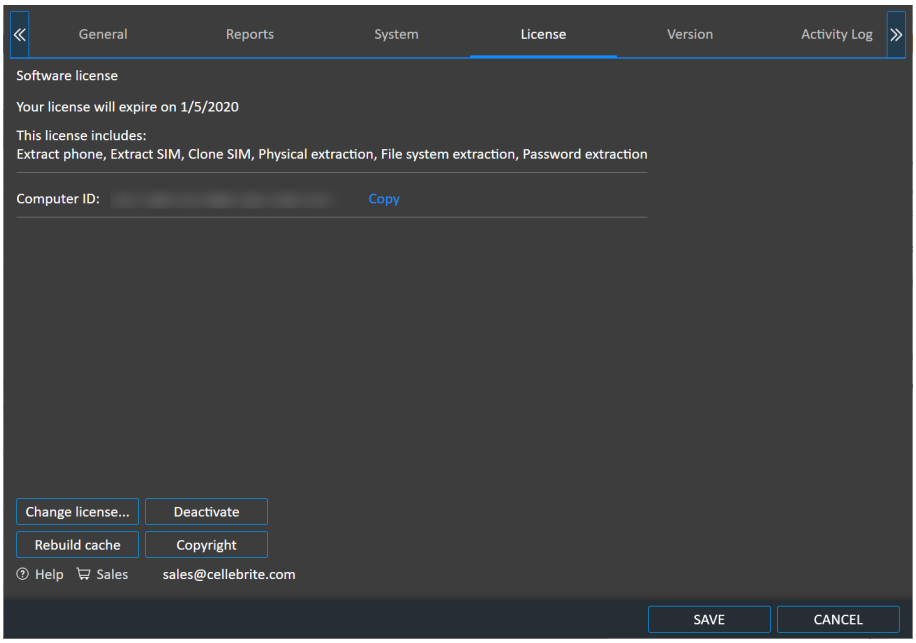
2. Select your license type.

6.4.2. Updating a dongle license online

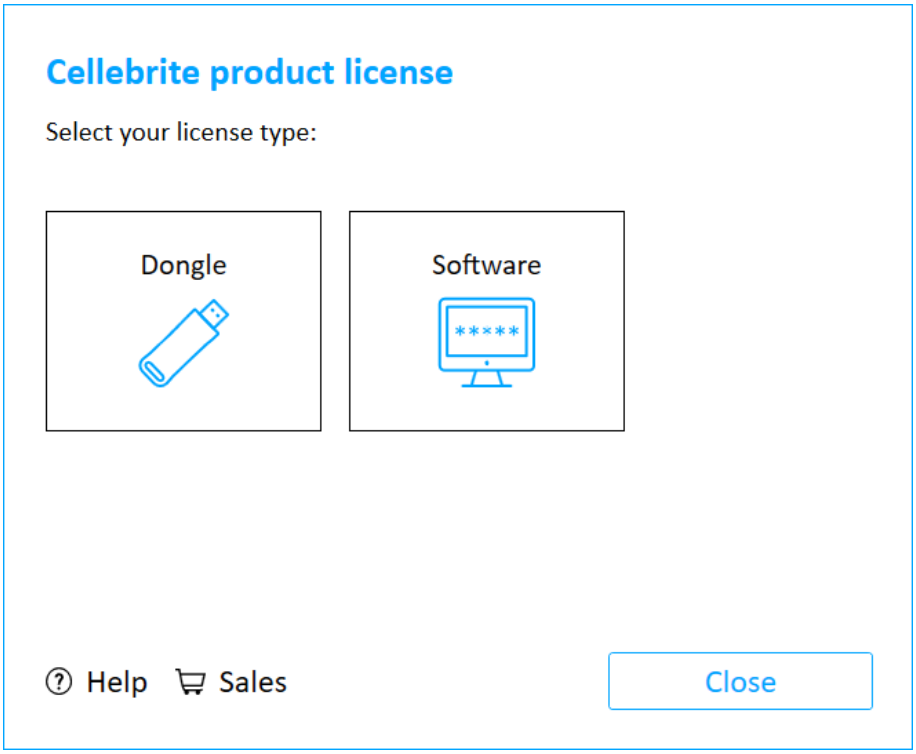
When an Internet connection is available, you can update the dongle license directly from Cellebrite Responder.

To update a dongle license online:

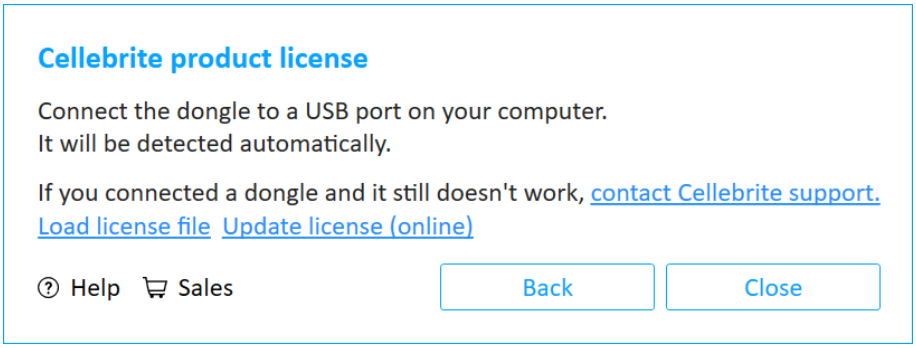
1. Contact your Cellebrite sales representative to renew or update the dongle license. Once the license is approved, you can then proceed with the following steps.
2. From the Home screen, tap  and then tap the License tab. The following window appears.



3. Tap **Change license**. The following window appears.



4. Tap **Dongle**. The following window appears.



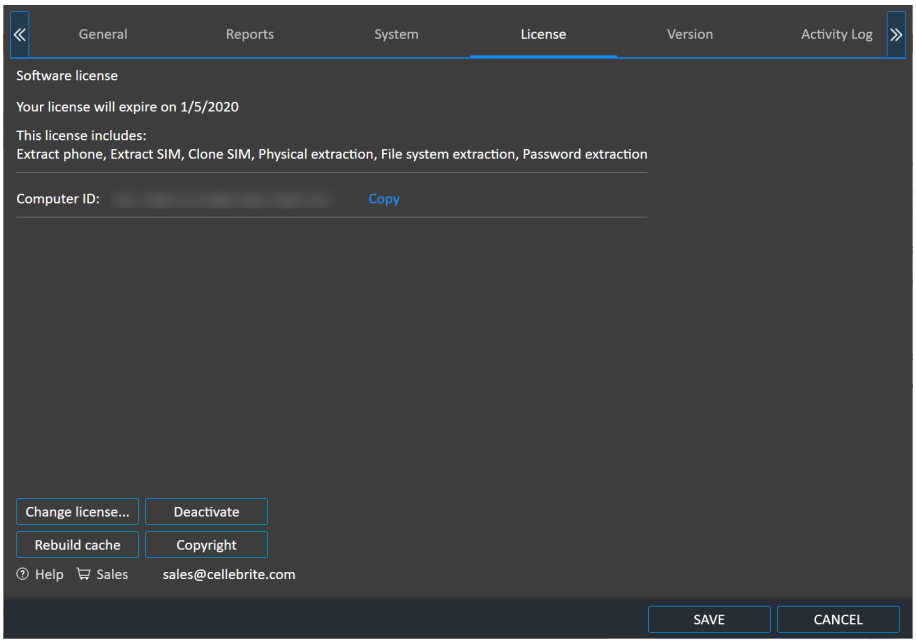
5. Tap **Update license (online)**.
6. Tap OK to complete the process.

6.4.3. Updating a software license online

When an Internet connection is available, you can update a software license directly from Cellebrite UFED.

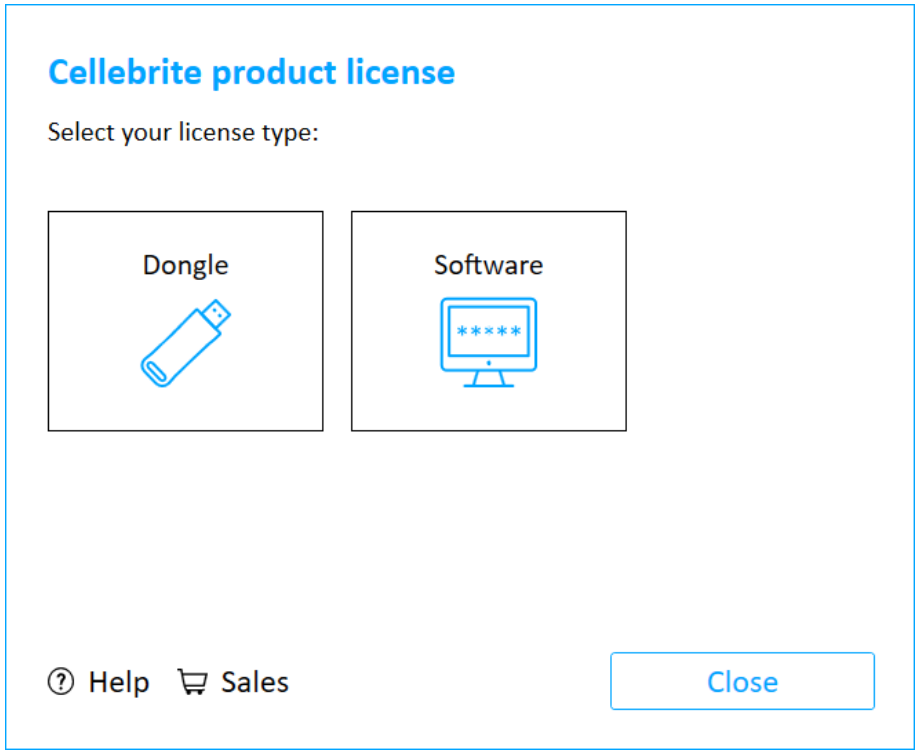
To update a software license online:

1. Contact your Cellebrite sales representative to renew or update the dongle license. Once the license is approved, you can then proceed with the following steps.
2. From the Home screen, tap  and tap the **License** tab. The following window appears.

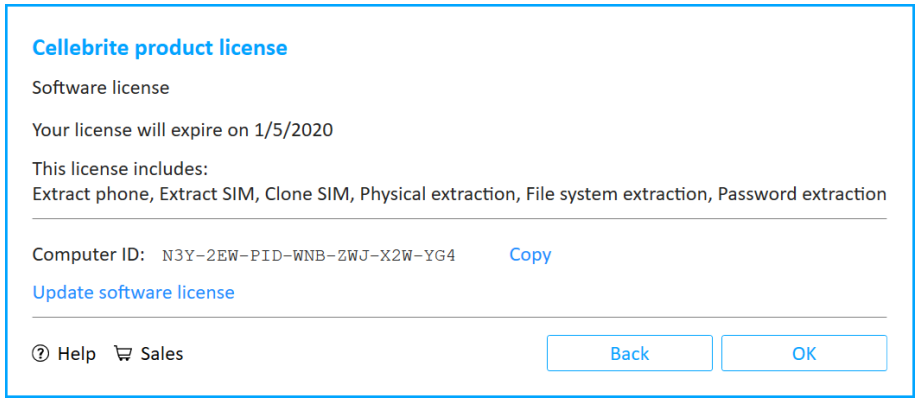


3. Tap **Change license**. The following window appears on Cellebrite Responder.

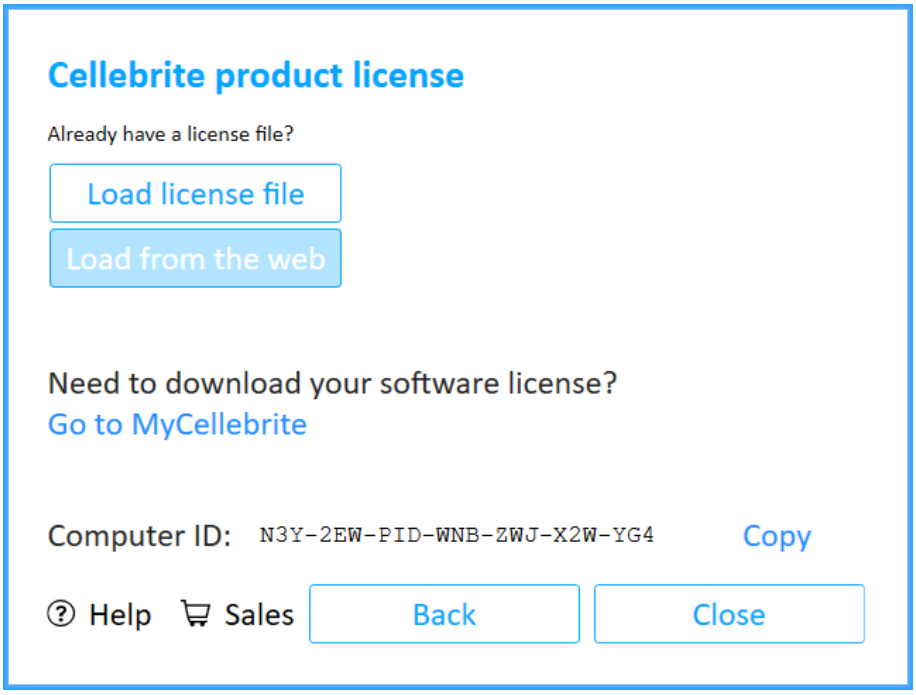
> For Cellebrite UFED Touch, accept the Cellebrite UFED License Agreement and skip to step 6.



4. Tap **Software**. The following window appears.



5. Tap **Update software license**. The following window appears.

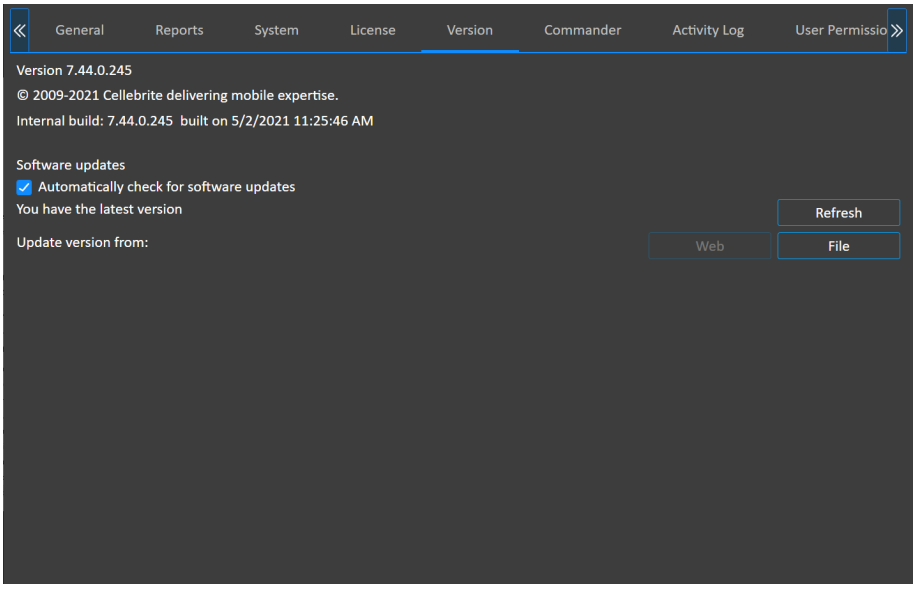


6. Tap **Load from the web**.
7. Tap OK in the Cellebrite product license window to complete the process.

6.5. Version details

The version tab displays information about the Cellebrite Responder version and build.

Under Software updates, select the check box to automatically check for software updates.



6.5.1. Updates and versions

When Cellebrite Responder is connected to the Internet, automatic notifications appear in the event of updates and new versions of the application.

» Click **Refresh** in the Settings > **Version** tab to update the information available on the screen.

To install a newer version of the Cellebrite Responder application via the web:

Before using this option, ensure that the unit is connected to the network.

» In the **Settings** > **Version** tab, in the **Version** area, click **Web**.

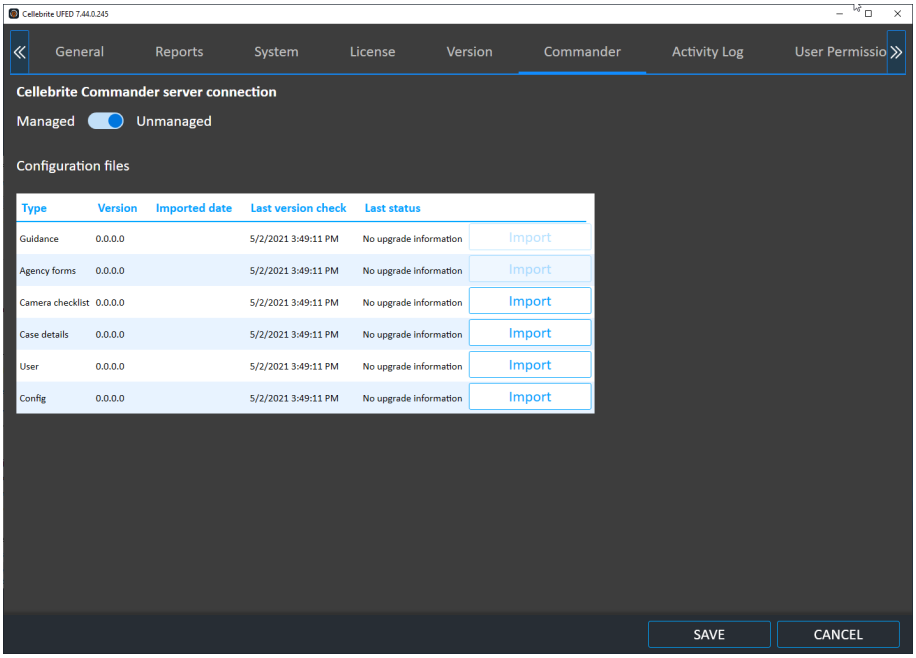
The application is upgraded to the latest version available on the Cellebrite Commander (if relevant) or Cellebrite download server.

To install a newer version of the Cellebrite Responder application using the file option:

1. Download the latest application version from your account in MyCellebrite, and save it to the specified directory on the PC or external device.
2. In the **Settings** > **Version** tab, in the **Version** area, click **File**.
3. Select the directory where you saved the file and then click **Open**.

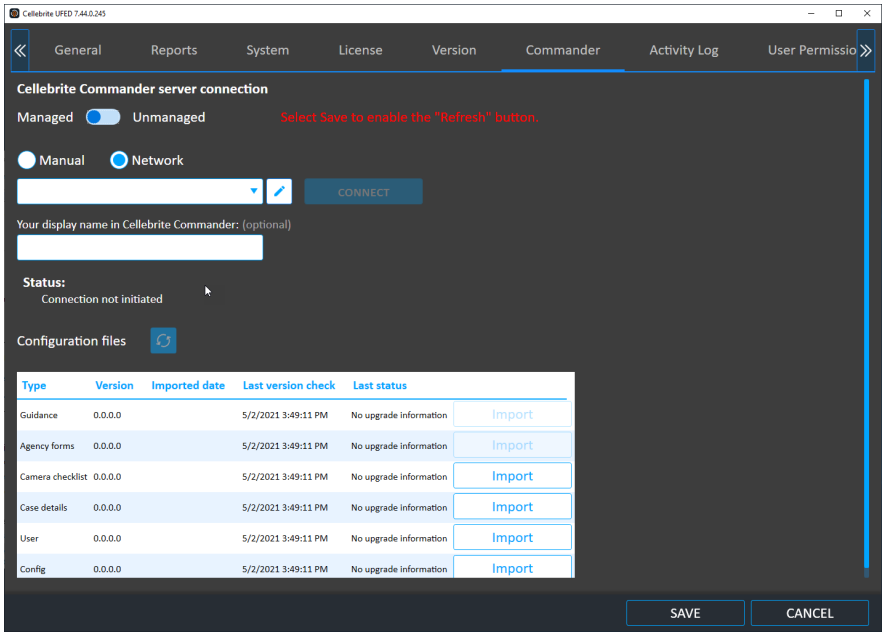
6.6. Commander settings

This tab can be used to manage and control deployed devices and systems via Cellebrite Commander. For more information, refer to the Cellebrite Commander *manual*.



If your organization is using Cellebrite Commander:

» Tap**Managed mode**.



For more information on setting up connectivity with Cellebrite Commander, see Connect a Cellebrite UFED device to Cellebrite Commander (on the next page).

Cellebrite Responder checks for configuration file changes by default every 5 minutes.

If you are not using Cellebrite Commander:

» Verify that **Unmanaged mode** is selected.

You can also manually import configuration and settings files into the system and check for software updates.

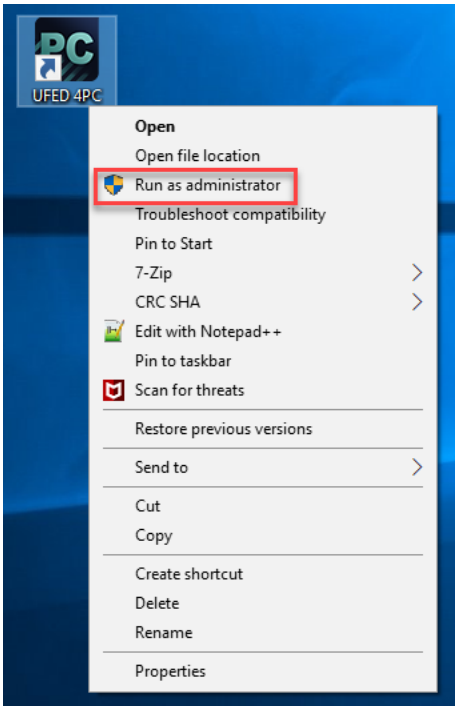
For more information on manually importing files, see Importing settings and configuration files (on page 109).

6.6.1. Connect a Cellebrite UFED device to Cellebrite Commander

Cellebrite UFED devices will automatically detect when a new Cellebrite Commander server is added to their subnet and prompt the user to connect automatically. If necessary, it is also possible to connect a Cellebrite UFED device to Cellebrite Commander manually.

To connect a Cellebrite UFED device to Cellebrite Commander automatically:

1. Preliminary step (Only applies to Cellebrite UFED 4PC and Cellebrite Responder on a PC): Right-click on the application shortcut and select **Run as Administrator**



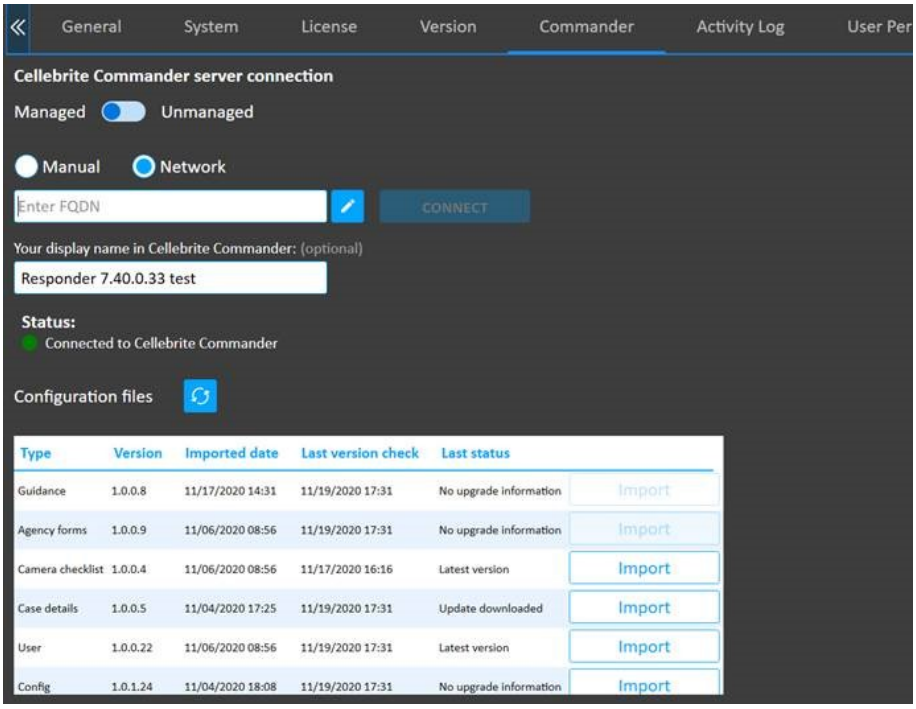
> Enable Admin permissions in order to allow the Cellebrite UFED device to automatically download the SSL certificate. This will ensure secure SSL communication between a managed Cellebrite UFED unit and Cellebrite Commander server. To enable the download of certificates, make sure the setting is enabled in Cellebrite Responder Settings.

2. Restart the Cellebrite UFED unit.
3. The unit will automatically detect the Cellebrite Commander server and prompt the user to connect.
4. After the unit connects to the Cellebrite Commander server, it will automatically switch to managed mode and download the secure SSL certificate.

If more than one Cellebrite Commander is detected, the user can choose from the list of servers.

To connect a Cellebrite UFED device to Cellebrite Commander manually:

1. Go to **Settings** > **Commander**. The following window appears.



2. Select **Managed mode**.
3. Enter the FQDN (fully qualified domain name).
4. Tap **Connect**. If the validation is successful, the status changes to **Connected to Cellebrite Commander** .
5. Tap **Save**.

6.6.2. Importing settings and configuration files

You can use Cellebrite Commander to download initial export files, which can then be edited if necessary and manually imported into Cellebrite Responder. These files can also be set using Cellebrite Commander. For more information, refer to the Cellebrite Commander manual.

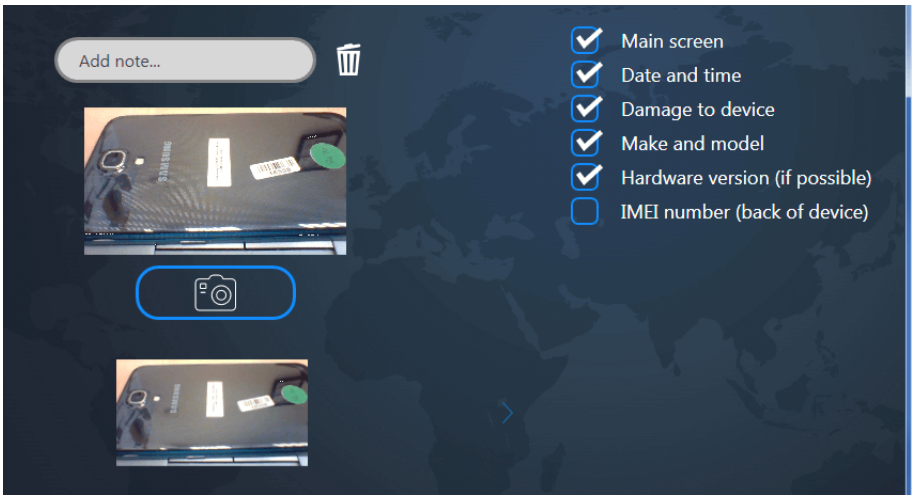
Cellebrite Responder can import the following type of settings and configuration files:

- Importing a camera checklist (on the facing page)
- Importing case details (on page 111)
- Importing Watch lists (on page 113)
- Importing user management (on page 115)
- Importing configuration files (on page 116)

6.6.2.1. Importing a camera checklist

The camera checklist enables you to upload an XML file that the user can use as a reference as to what pictures are required of the device. As the user completes each step, they can place a check mark next to the completed items.

An example is displayed next.



To manually import a Camera checklist file:

1. In the **Version** tab, tap the **Import** button next to the setting file you would like to import. The following window appears.
2. Browse to the relevant file and tap **Open**.
3. Tap **OK** to update the application.

The following example shows the structure of the XML file.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CheckListData>
    <Version>1.0.0.48</Version>
    <CheckListItems>
        <CheckListItem>Main screen</CheckListItem>
        <CheckListItem>Date and time</CheckListItem>
        <CheckListItem>IMEI number</CheckListItem>
    </CheckListItems>
</CheckListData>
```

6.6.2.2. Importing case details

You can import an XML file to change the options that appear in the Case Details window (see Case details (on page 36)).

To manually import a case details file:

1. In the Version tab, click the **Import** button next to the setting file you would like to import.
2. Browse to the relevant file and click **Open**.
3. Tap OK to update the application.

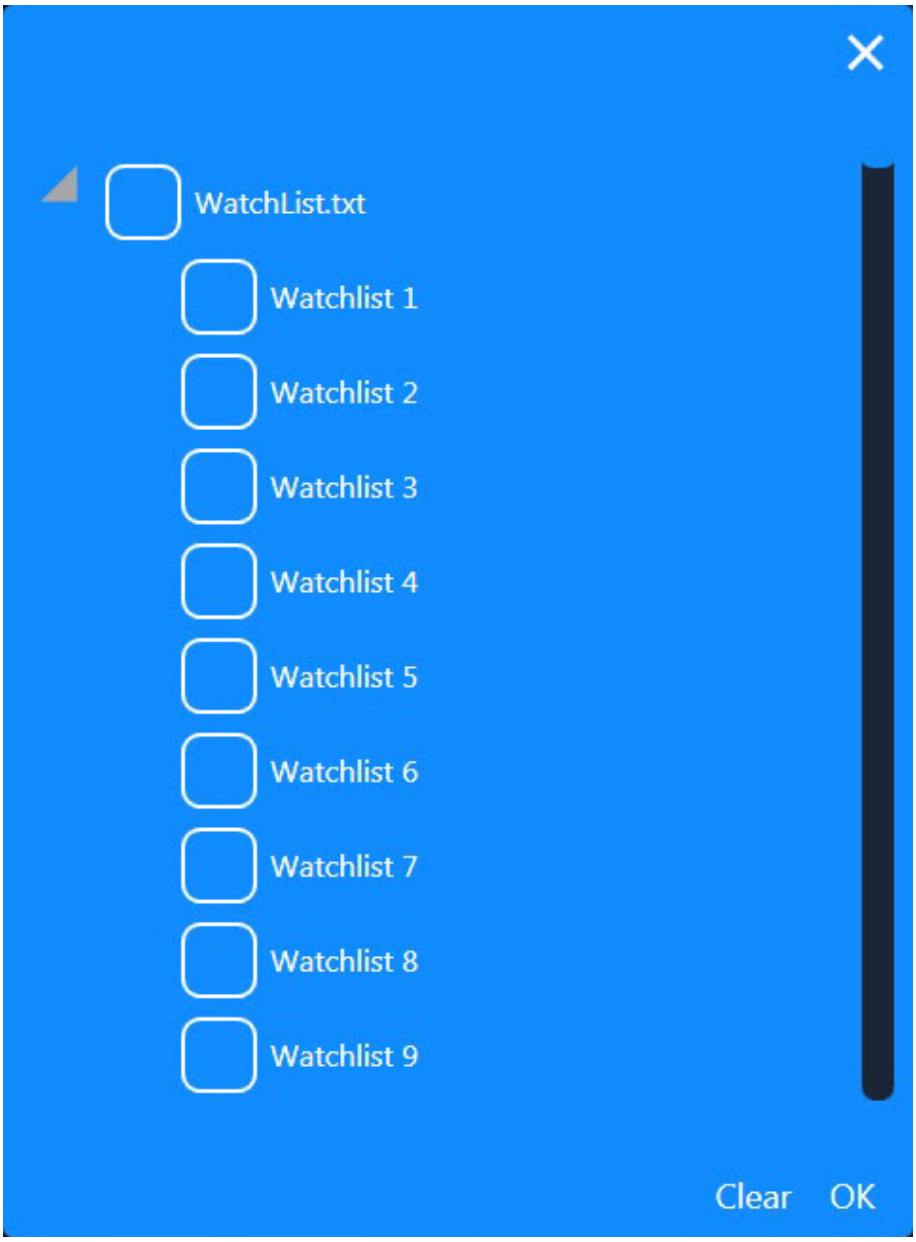
The following example shows the structure of the XML file.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CaseDetails>
    <Version>1.0.0.38</Version>
    <Fields>
        <Field>
            <Type>String</Type>
            <Caption>Case ID</Caption>
            <Mandatory>true</Mandatory>
            <AutoFill>true</AutoFill>
            <IsDefaultFolderName>true</IsDefaultFolderName>
        </Field>
        <Field>
            <Type>String</Type>
            <Caption>Seized by</Caption>
            <Mandatory>false</Mandatory>
            <AutoFill>false</AutoFill>
            <IsDefaultFolderName>false</IsDefaultFolderName>
        </Field>
        <Field>
            <Type>String</Type>
            <Caption>Crime type</Caption>
            <Mandatory>false</Mandatory>
            <AutoFill>false</AutoFill>
            <IsDefaultFolderName>false</IsDefaultFolderName>
            <Values>
                <Value>Armed Robbery</Value>
                <Value>Attempted Murder</Value>
                <Value>Child Exploitation</Value>
            </Values>
        </Field>
        <Field>
            <Type>String</Type>
            <Caption>Device owner</Caption>
            <Mandatory>false</Mandatory>
            <AutoFill>false</AutoFill>
            <IsDefaultFolderName>false</IsDefaultFolderName>
            <Values>
                <Value>Victim</Value>
                <Value>Suspect</Value>
                <Value>Witnesss</Value>
            </Values>
        </Field>
    </Fields>
</CaseDetails>
```

6.6.2.3. Importing Watch lists

An XML watch list, needs to be imported into Cellebrite Responder before it can be used.

When a watch list is imported, it will be available for use as a filter following an extraction. An example is displayed next.



To manually import a Watch list file:

1. In the **Version** tab, tap the **Import** button next to the setting file you would like to import.
2. Browse to the relevant file and tap **Open**.
3. Tap **OK** to update the application.

The following example shows the structure of the XML file.

```
<?xml version="1.0" encoding="UTF-8"?>
<WatchListRoot xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<version>1.0.0.18</version>
<WatchLists>
    <WatchList Title="DrugWatchlist" SortOrder="0">
        <Configuration>
            <Config></Config>
        </Configuration>
            <Items Id="334">
                <Item Id="85">Drug </Item>
                <Item Id="88">Sugar</Item>
                <Item Id="89">white</Item>
                <Item Id="90">package</Item>
                <Item Id="91">blue</Item>
                <Item Id="92">chocolate</Item>
                <Item Id="93">sweet</Item>
            </Items>
        </WatchList>
    </WatchLists>
</WatchListRoot>
```

6.6.2.4. Importing user management

Cellebrite Commander enables user authentication ensuring that only users with the right credentials can access the application. Access rights are further enforced by defining permission levels per profile.

To manually import a user management file:

1. In the **Version** tab, select the **Import** button next to the setting file you would like to import.
2. Browse to the relevant file and tap **Open**.
3. Tap **OK** to update the application.

6.6.2.5. Importing configuration files

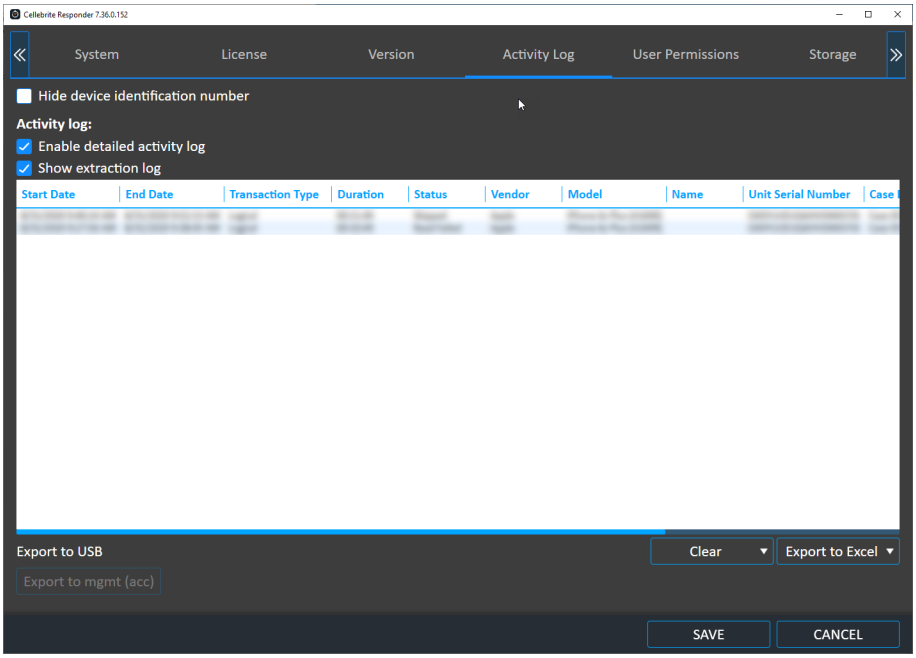
Configuration files enables you to import various settings into the system.

To manually import a configuration file:

1. In the **Version** tab, select the **Import** button next to the setting file you would like to import.
2. Browse to the relevant file and tap **Open**.
3. Tap **OK** to update the application.

6.7. Activity Log

The Activity Log lists all transactions performed by Cellebrite Responder. It includes information such as when the extraction started and ended, transaction type, duration, status, device vendor, device model, name, serial number of Cellebrite Responder, case ID, crime type, device owner, and who seized the device. You can also clear the activity log, export the activity data to a CSV file and show or hide the activity data.



6.7.1. Detailed activity log

Cellebrite Responder can log each action performed by the user to provide admins with better traceability and control.

The detailed activity log will include records on every option chosen or button clicked to audit the full user journey.

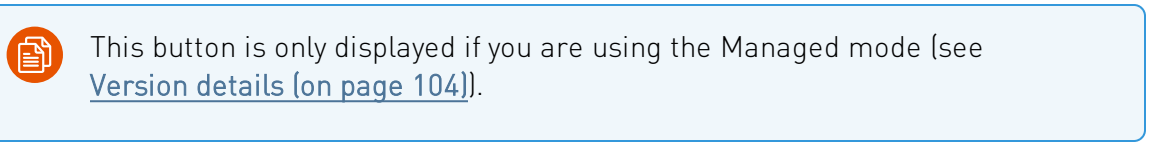
When selecting the **Enable detailed activity log** check box, this data will be included in the export.

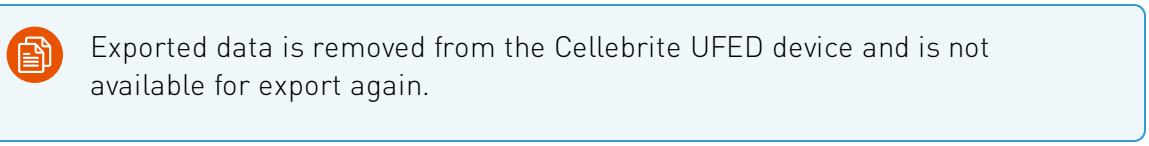
6.7.2. Exporting metadata to Cellebrite Commander

If a Cellebrite UFED unit is used in an offline environment, you can export the usage metadata file. This file contains the following: Cellebrite UFED device information (e.g., MAC address, serial number, software version number), transaction start times and end times, source phone information (e.g., vendor, model name, IMEI, and OS), and type of information extracted (e.g., Phone memory, SMS memory, MMS, pictures, videos, audio). The exported Zip file can then be manually imported into Cellebrite Commander. For more information, refer to the Cellebrite Commander manual.

To export the metadata:

1. Connect or reconnect a USB flash drive to the Cellebrite UFED unit. The button is only available when a USB drive is connected.
2. Tap the **Export to mgmt (acc)** button. The metadata can now be imported into Cellebrite Commander.

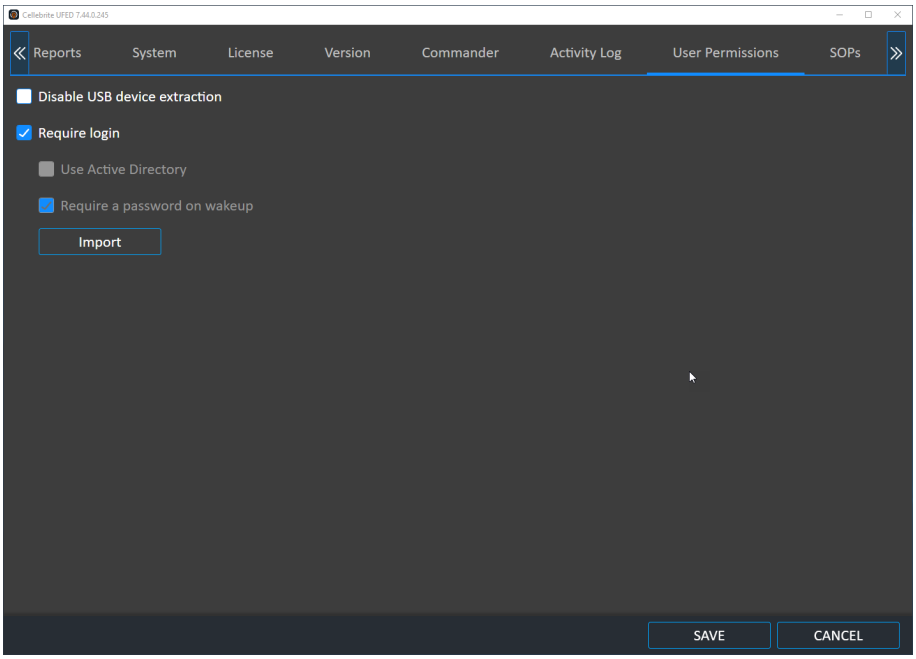




6.8. Users permissions

Define and configure user authentication settings to ensure that only users with the right credentials can access the application. Access rights are further enforced by defining permission levels per profile.

User permissions can be set using Cellebrite Commander (refer to the Cellebrite Commander *manual*) or the UFED Permission Manager (see Permission management (on page 127)).

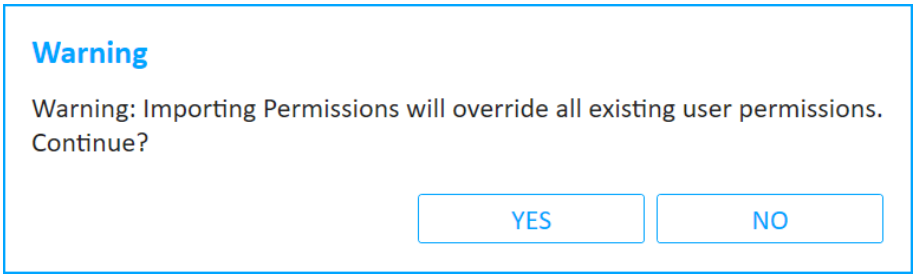


To disable USB device extraction:

» Select the **Disable USB device extraction** check box. The USB device option will not be available on the home screen.

To import user permissions:

1. Run the Cellebrite Responder as an administrator.
2. Click Import. The following warning appears.



3. Tap **Yes** and navigate to the directory where the permission management file (*.cp) is located. For information on creating a permission management file, see Using the Cellebrite UFED Permission Manager (on page 127).
4. Tap **Open** and then tap **Save**.
5. Restart the Cellebrite Responder application, which will now prompt for login credentials.
6. Use one of the login credentials configured in the permission management file. For more information, see Permission management (on page 127).

Select the check box to require password on wakeup.

6.8.1. Active Directory integration

Active Directory is a Microsoft product providing a range of directory-based identity-related services. It authenticates and authorizes all users and computers in a Windows domain type network, assigning and enforcing security policies for all computers and installing or updating software.

When a user logs in to the system, Active Directory checks the submitted password and determines whether the user is a system administrator or normal user before allowing the user to log in. Active Directory also enables the management and storage of information at the admin level and provides authentication and authorization mechanisms.

Use the Windows Active Directory account to enable *quicker and easier* login to your Cellebrite UFED applications. Cellebrite UFED can manage the permissions with two permissions levels:

- Active Directory Groups
- Active Directory Users with Commander roles

6.8.1.1. Determining the Active Directory groups

When using the **Groups level**, the permissions are applied according to the Active Directory groups of which the users are members (directly and indirectly). When using the **Users level**, you first need to map the users to Cellebrite Commander, and then to the permissions applied according to the selected profile in Cellebrite Commander. For more information, see To enable Active Directory (on page 122).

If required, use the following procedure to determine all the Active Directory groups for a specific user.

1. To get a list of groups for a specific user, replace the **USERNAME** with the actual user name

   Open up a command prompt (cmd.exe) and run:

`gpresult /V /user USERNAME`

2. The output will look like this (truncated with only the group info):

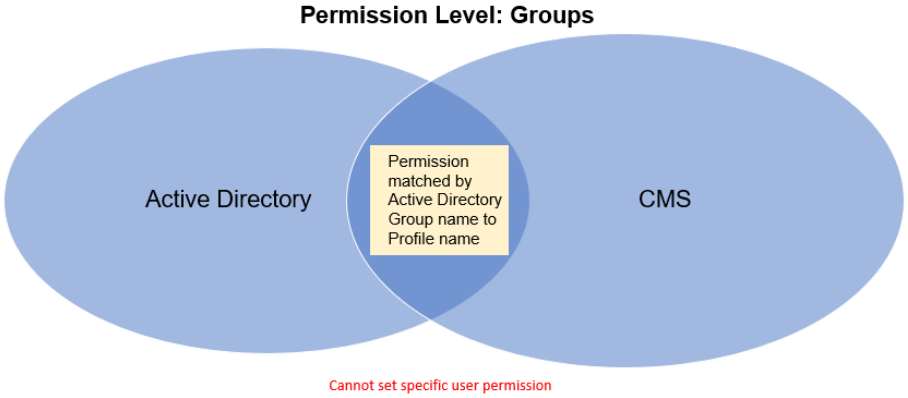
```
The user is a part of the following security groups

---------------------------------------------------

    Domain Users

    Everyone

    BUILTIN\Users

    NT AUTHORITY\INTERACTIVE

    CONSOLE LOGON

    NT AUTHORITY\Authenticated Users

    This Organization

    LOCAL

    Marketing
    Platforms Dev Team
```

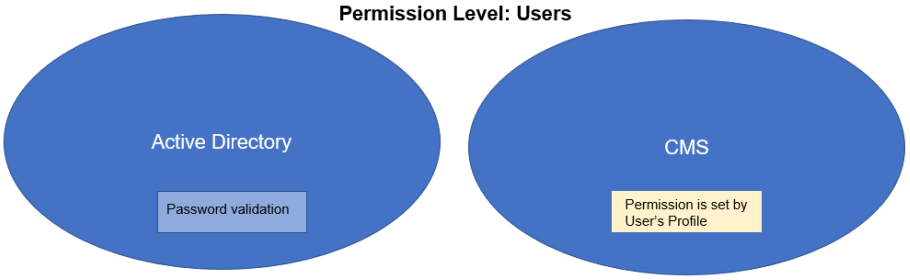
In the above example, you can see that this user is a member of several Active Directory (security) groups. In the following example we will use the "Platforms Dev Team" security group.

If a group is contained within another group, other commands (such as `whoami /groups`) will only display the groups of which the user is a direct member. Therefore, it is recommended to avoid `whoami` as an indicator.

6.8.1.2. Using Cellebrite Commander

When using Cellebrite Commander, the system administrator needs to decide the permission management level. The possible levels are presented below:





6.8.1.3. Initial setup

When Cellebrite Commander is used in conjunction with Active Directory, the following procedures are required for initial setup.

6.8.1.3.1. Permission Level – Groups

The Cellebrite Commander administrator needs to:

1. Create *profiles* with the exact same name of the relevant Active Directory groups.
2. Publish the users and permissions to all the relevant Cellebrite UFED units.

   Once Active Directory is set up, each login request via a Windows user will be sent to Active Directory before approval. Active Directory checks the user's permissions and notifies the Cellebrite UFED unit whether to approve or deny the login request based on the user profile permissions.

If the Cellebrite UFED units are offline, you will not be able to log in to the Cellebrite UFED unit. However, an ongoing session will not be disconnected if a disconnection occurred.

Should you choose not to work with Active Directory, the Cellebrite Commander administrator can regulate the users and permissions via Cellebrite Commander or the Cellebrite UFED Permission Manager.

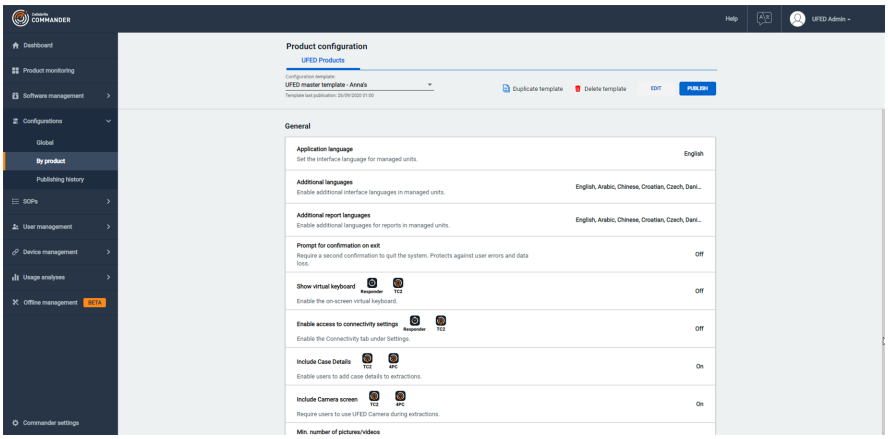
6.8.1.3.2. Permission Level – Users

The Cellebrite Commander administrator needs to:

1. Create *profiles* and set the permissions for each profile.
2. Import a CSV list of relevant *users* that matches the Users and Profiles settings in Cellebrite Commander.
3. Publish the users and permissions to all the relevant Cellebrite UFED units.

6.8.1.4. To enable Active Directory

1. In Cellebrite Commander select **Configurations > By product**. The following window appears.



2. Click **Edit**,to enable the following under the Access Control section:
   a. **Require login**.
   b. **Enable Active Directory integration**.

3. Under **Permissions level**, select one of the following options:
    - **Active Directory groups:** Manage permissions at the Active Directory groups level. The match is performed by Active Directory group names.
    - **Active Directory users with Commander roles:** Manage permissions per user independently from Active Directory groups.
4. Click **Save** to save the configuration template.
5. Publish the configuration template to the relevant product.

Next you need to add the Active Directory profile and select the required permissions.

6.8.1.4.1. To add a role and select permissions

Adding roles and selecting permissions are managed in the User Management System. For more information, see the Managing Roles section in the User Management System manual.

6.8.1.4.2. Adding Users

Adding users is managed in the User Management System. For more information, see the Managing Users section in the User Management System manual.

6.8.1.5. Logging in to Cellebrite UFED

Once Active Directory is enabled, the following will occur depending on the Cellebrite UFED device you are using.

- In PC applications such as Cellebrite UFED 4PC and Cellebrite Responder, the login will occur automatically when you start the Cellebrite UFED application.
- In closed systems such as Cellebrite UFED Touch and Kiosk, Cellebrite UFED tries to locate the domain and display the following login screen.

1. Enter the Active Directory credentials.
2. Verify the Domain field.

If the text in the "Domain" field (i.e., "domain controller host") is missing or incorrect, contact your IT department.

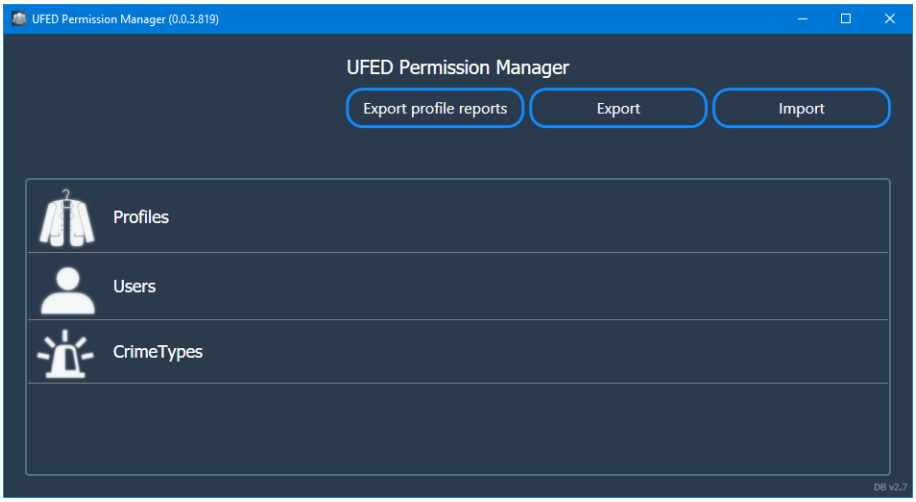
6.8.1.6. Cellebrite UFED Permission Manager

If you are not using Cellebrite Commander, use the following procedures in the Cellebrite UFED Permission Manager and Cellebrite UFED application to enable Active Directory.

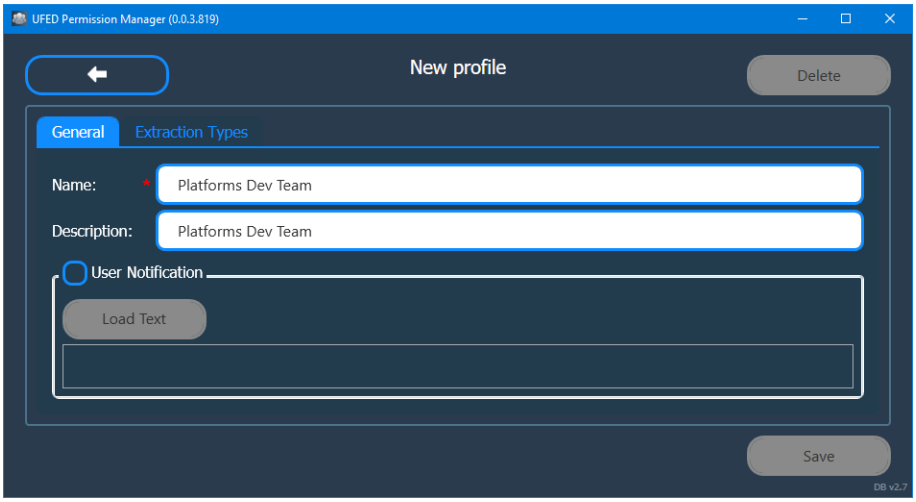
To configure Active Directory in the Cellebrite UFED Permission Manager:

In the Cellebrite UFED Permission Manager, create a profile that corresponds to the required Active Directory group.

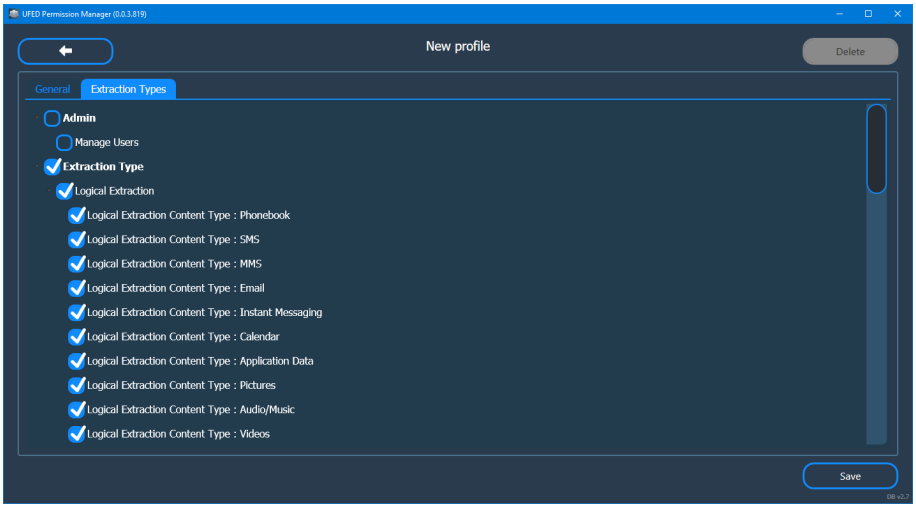
1. Run the Cellebrite UFED Permission Manager. The following window appears.



2. Click **Profiles** > **New Profile**. The following window appears.



3. In the Name field enter the name of the Active Directory group. i.e., Platforms Dev Team.
4. Enter a description (optional).
5. Click **Extraction Types** and enter all the required permissions for the profile. The following window appears.

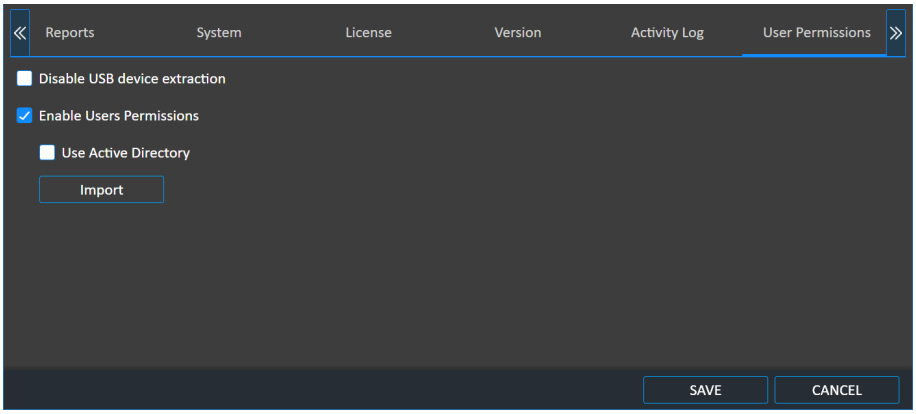


6. Click **Save**.

To enable Active Directory in the Cellebrite UFED application:

> This step is not required if you are using Cellebrite Commander.

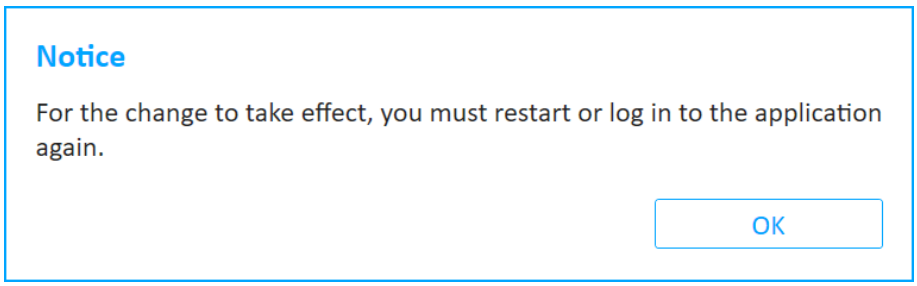
1. In Cellebrite UFED go to **Settings** > **User Permissions**.



2. Select **Use Active Directory**.

> You can only login to the application using Active Directory users, there will no longer be Cellebrite UFED users such as Manager and Investigator. After activating Active Directory either in Cellebrite Commander or Cellebrite UFED application.

3. Click **Save**. The following window appears.



4. Click OK and restart the Cellebrite UFED application.

For information on how to login to the Cellebrite UFED devices, see Logging in to Cellebrite UFED (on page 124).

6.8.2. Permission management

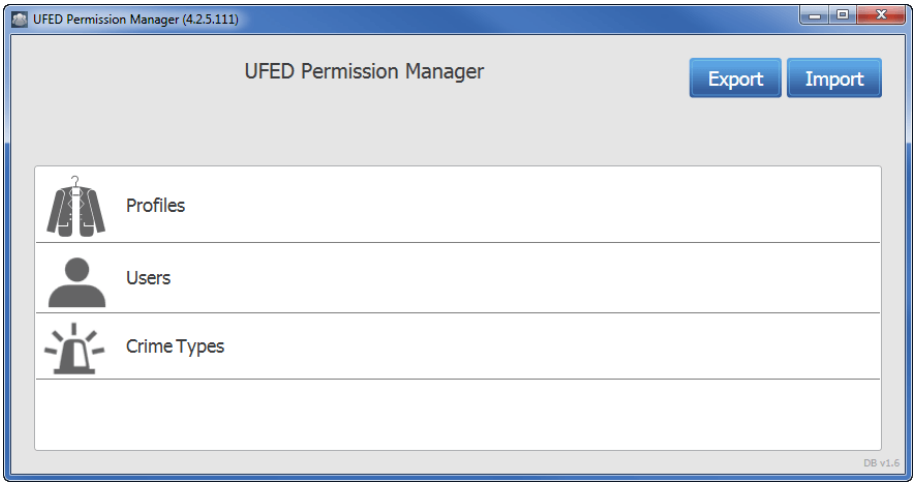
Permission management can be performed via Cellebrite Commander or the Cellebrite UFED Permission Manager standalone application.

The Cellebrite UFED Permission Manager standalone application is available from MyCellebrite. Each profile contains access permissions, including operation rights per extraction type and content types. A single profile can be assigned to multiple users. The users and profiles can be exported into an encrypted permission management file, which can be imported into multiple Cellebrite Responder applications.

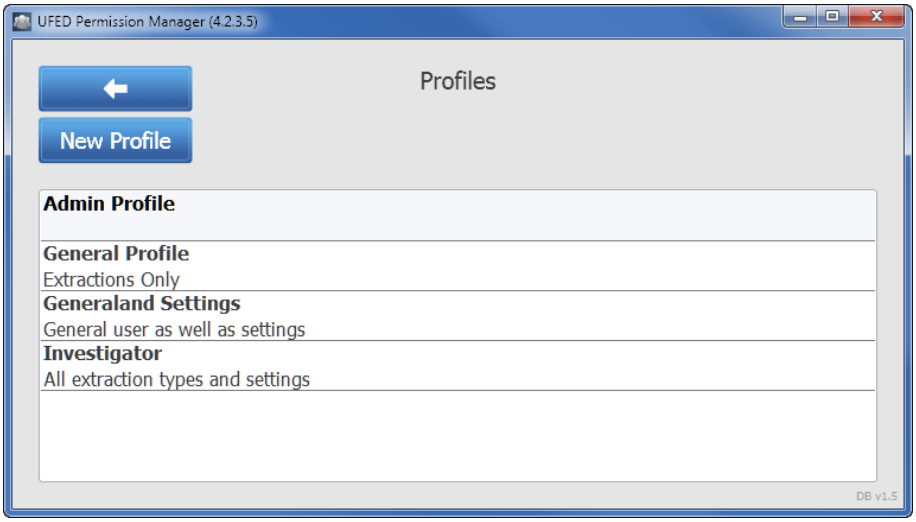
6.8.2.1. Using the Cellebrite UFED Permission Manager

To create a new profile:

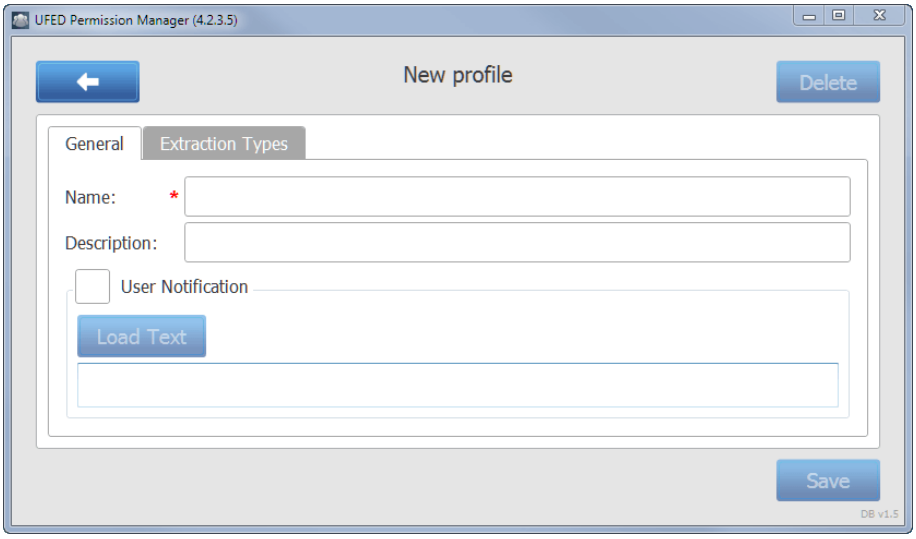
1. Download the latest Cellebrite UFED Permission Manager application from your account in MyCellebrite, and save it to a directory on a computer or external device.
2. Run the Cellebrite UFED Permission Manager and follow the setup instructions. The Cellebrite UFED Permission Manager screen appears.



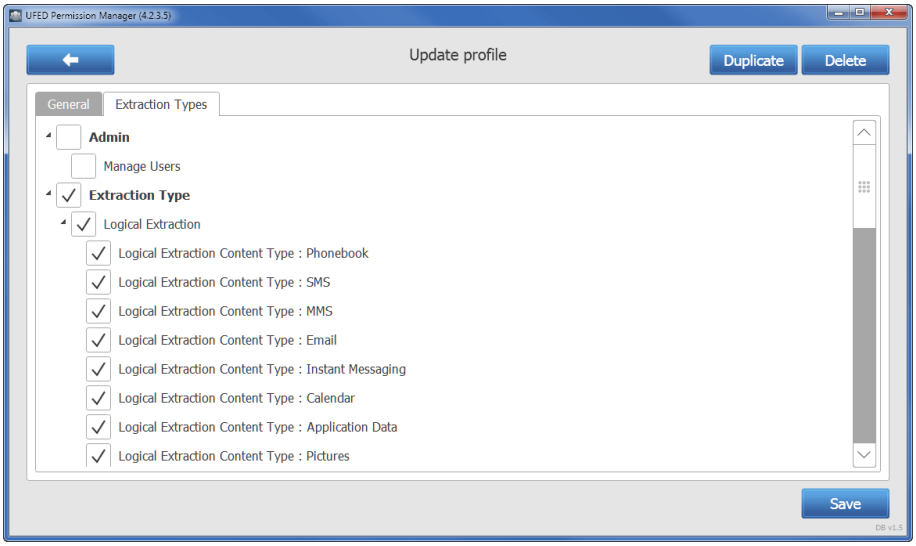
3. Tap **Profiles**.



4. Tap **New Profile**. The following screen appears.



5. Enter a name and description for this profile.
6. If required select the **User Notification** check box, which enables you to load a RTF file with text and graphics for the profile.
7. Tap the **Extraction Types** tab.



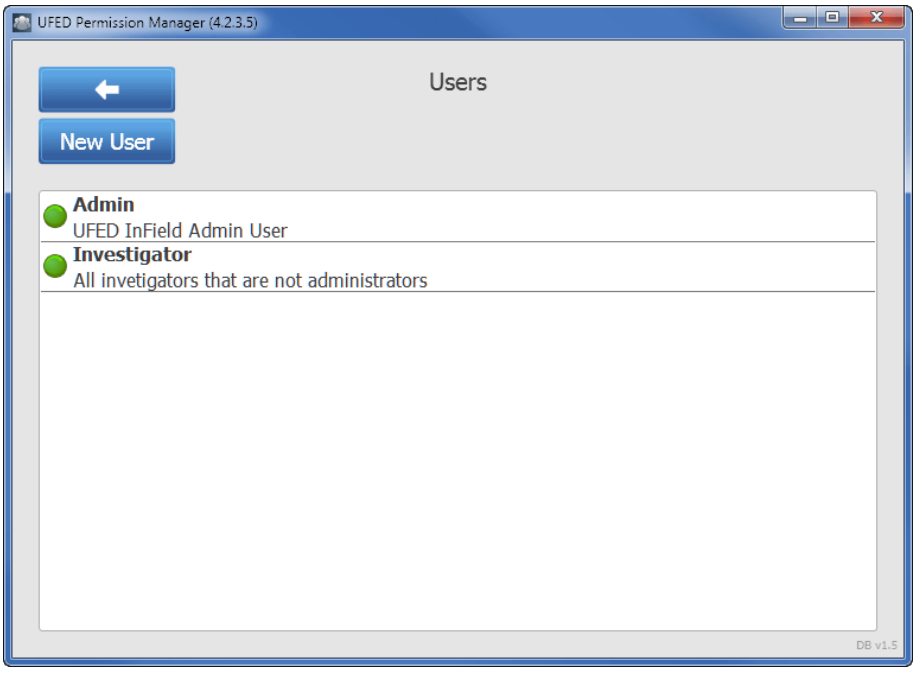
8. Select the options for this profile, such as Admin who can manage users, the Extraction Type (Logical Extraction, SIM Data extraction, Password extraction etc.) and UFED Settings (Activity Log).

> At least one of the enabled users must be an Administrator (Admin).

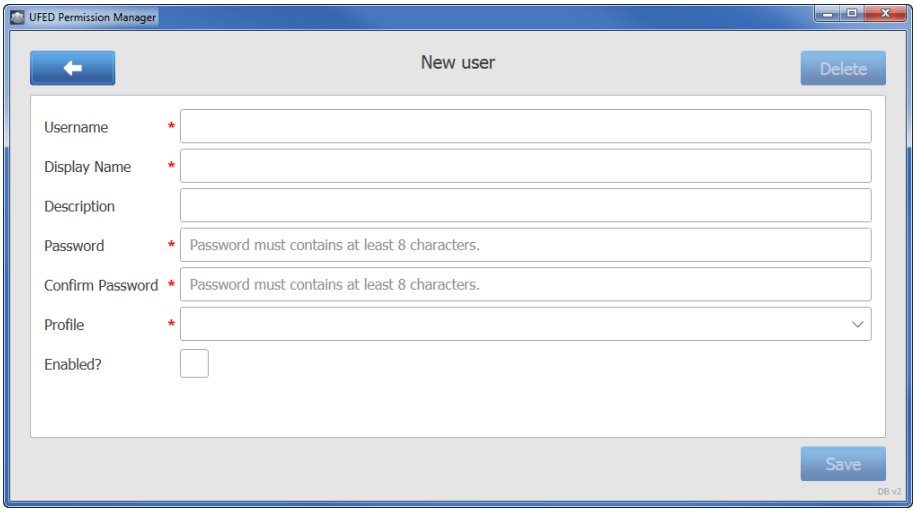
9. Tap **Save** and proceed to create a new user.

To create a new user:

1. In the Cellebrite UFED Permission Manager screen, tap **Users**. The following screen appears.



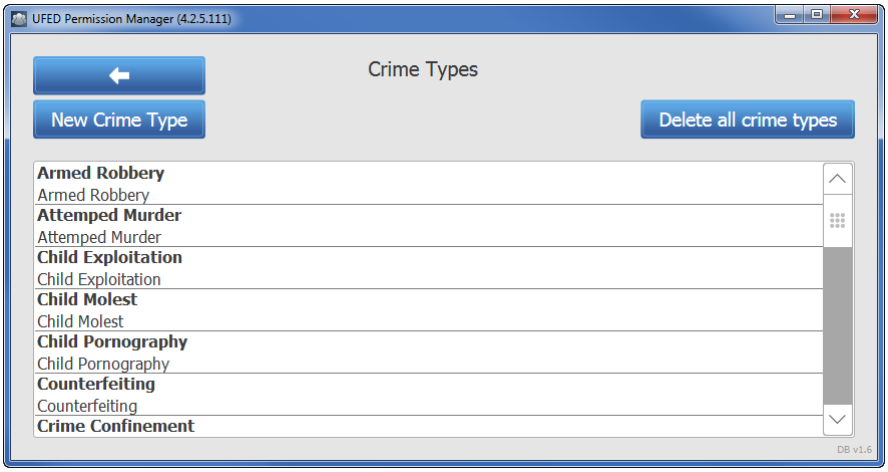
2. Tap **New User**. The following screen appears.



3. Enter the details for the new user including Username, Display Name, Description, and Password.
4. Select a profile for the user.
5. Select **Enabled** to enable the user.
6. Tap **Save**.

To manage crime types:

1. Tap **Crime Types**. The following screen appears.

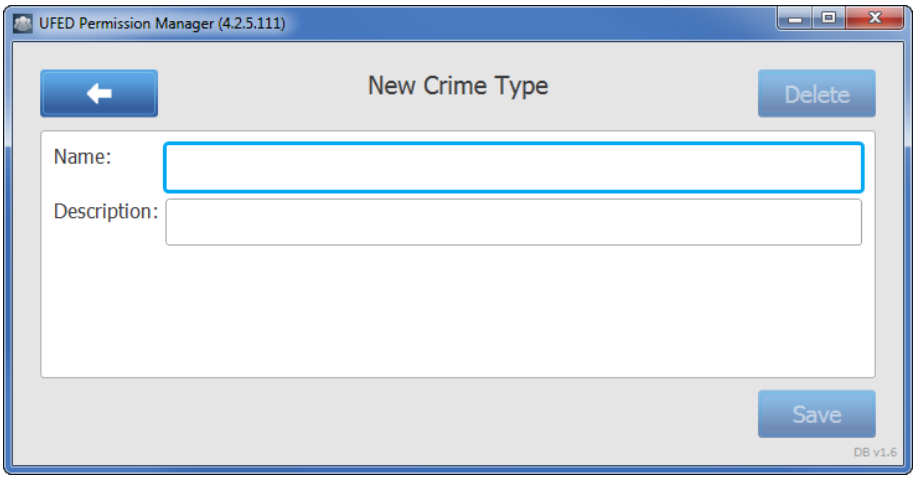


The crime types are only relevant for Cellebrite Responder.

You can delete all crime types; however you must add at least one crime to be able to export a permission management file.

To edit a crime type, click the crime type and edit the Name.

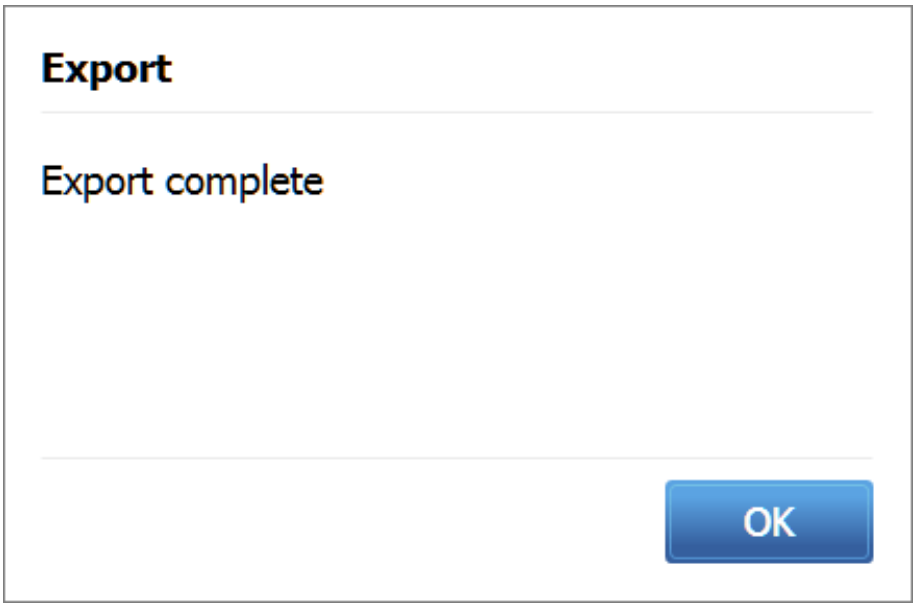
2. Tap **New Crime Type**. The following window appears.



3. Enter a name for the crime type and a description (optional).
4. Tap **Save**.

To export an encrypted permission management file:

1. In the Cellebrite UFED Permission Manager screen, tap **Export**, specify a directory for the file and tap **Save**. The following screen appears.



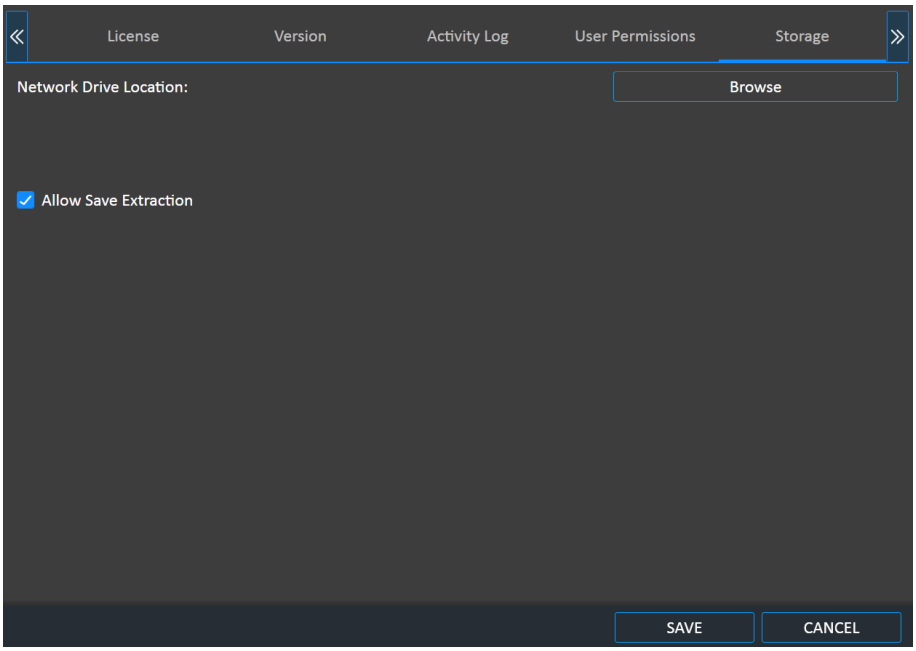
2. Tap OK. The permission file must be imported into Cellebrite Responder via the User Permissions tab in the Settings window.

> The next time you run the Cellebrite UFED Permission Manager you will be prompted for your user credentials to access the application.

6.9. Storage

This window can be used to specify a network location, or to change the default parent folder name where reports or extracted data are saved.

Storage settings can also be specified in Cellebrite Commander.



To specify a network location:

1. Tap **Browse** and navigate to the network location.
2. Tap OK.

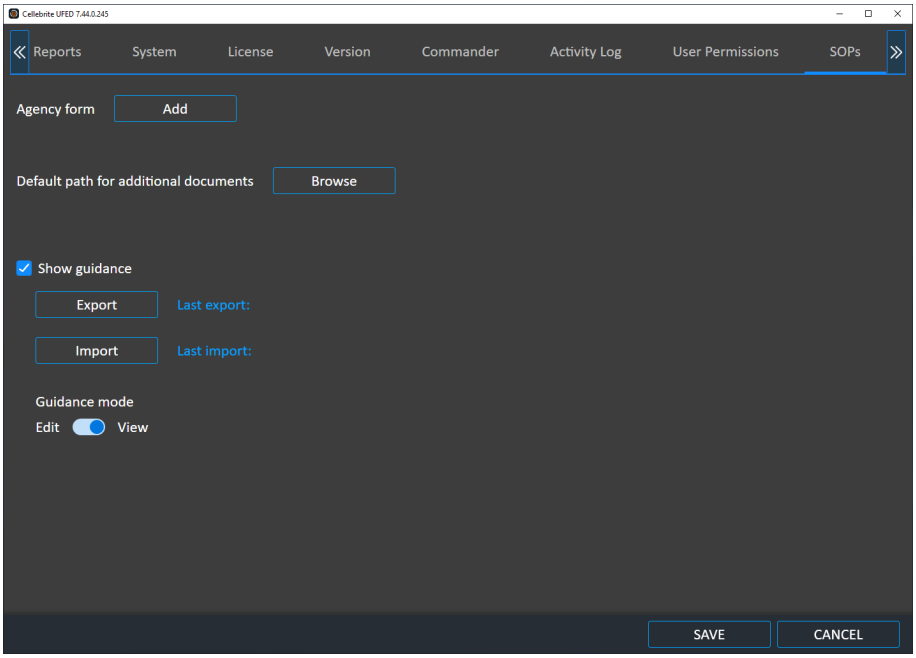
   On the Kiosk, the **Open File Browser** option opens a browser window.

   In a situation when a Network drive location has not or cannot be defined, use the **Open File Browser** option to find an extraction on the network.

6.10. SOPs

In the Settings > SOPs, you can manage the following:

- Adding Agency forms.
- Setting a default path for additional documents.
- Managing Workflow guidance. See Workflow guidance settings (on page 139).



6.10.1. Agency forms

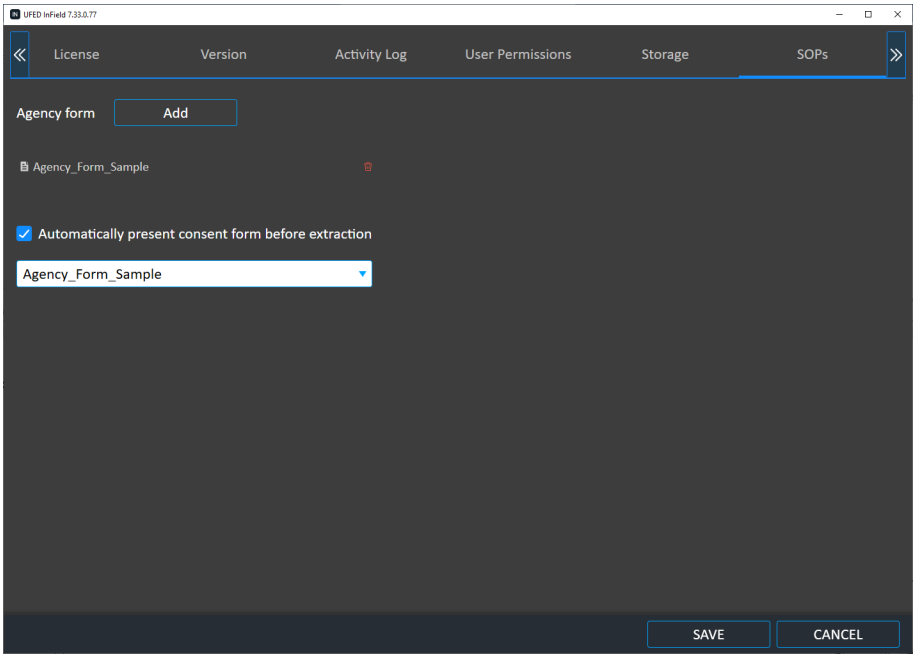
The Agency form feature enables an administrator to multiple customizable forms to be completed and signed as part of the Cellebrite Responder workflow (e.g., consent form). To collect digital data, user consent is mandatory in some jurisdictions. With digital consent forms, the subject can view and sign the consent form before, during, and after data collection. Signed forms will be automatically saved with your case and collected data.

If the **Automatically present consent form before extraction** check box is selected, the form appears during the extraction after the Case Details are completed.

To access agency forms at any time during the extraction flow click  at the top of the screen.

To add an agency form:

1. Go to settings > **SOPs**. The following window appears.



2. Click **Add**.
3. Select the Agency form file.
4. To present a form before extraction select the **Automatically present consent form before extraction** check box and select the form from the dropdown list.

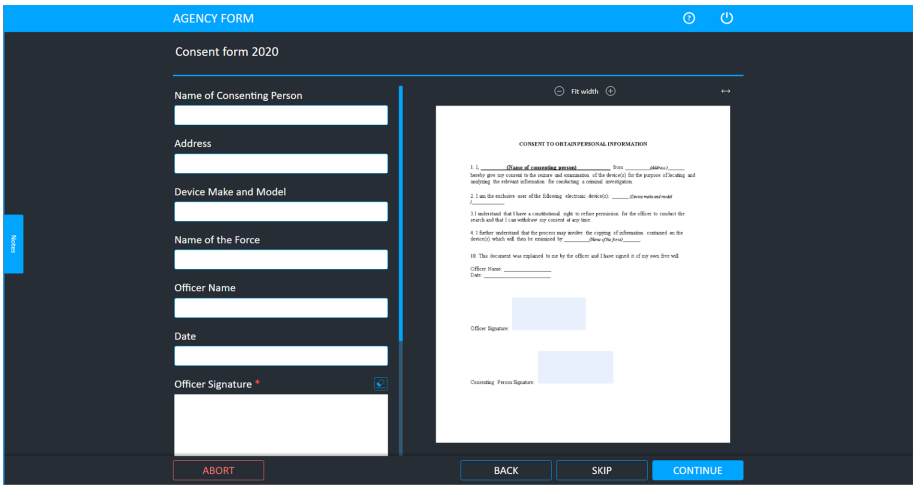
The window indicates if the form was uploaded successfully and the fields specified in the form.

> To be able to upload a form it must be created using Microsoft Word Controls and conform to a number of rules. For more information, see Agency form rules (on the facing page).

5. Click **Save**.

To use the agency form that was selected to be automatically presented:

1. Start an extraction and complete the Case Details. The selected agency form is displayed next.

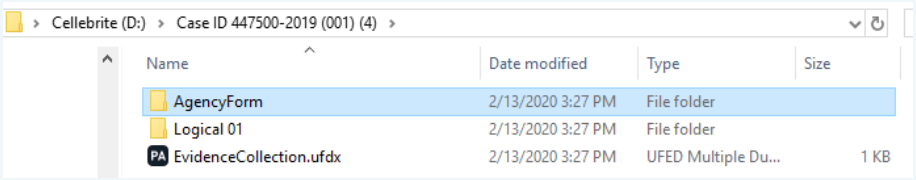


2. Complete the details in the form.
3. If required, click **Abort** to end the extraction, **Back** to go back to the previous step or **Skip** to skip the form. Any information entered into the form will be lost.

> You can use the buttons above the form to resize or the fit the form on the screen.

4. Sign the form and click **Continue**. Signature fields are optional.

> After completing the extraction, the form will be displayed as a PDF file in the AgencyForm folder when the report or extraction is saved.



6.10.1.1. Agency form rules

The Agency form feature supports Microsoft Word forms. It uses Content Controls, which are individual controls that you can use to add and customize forms. Different styles can be used for the input text. The form must be saved as *.docx format.

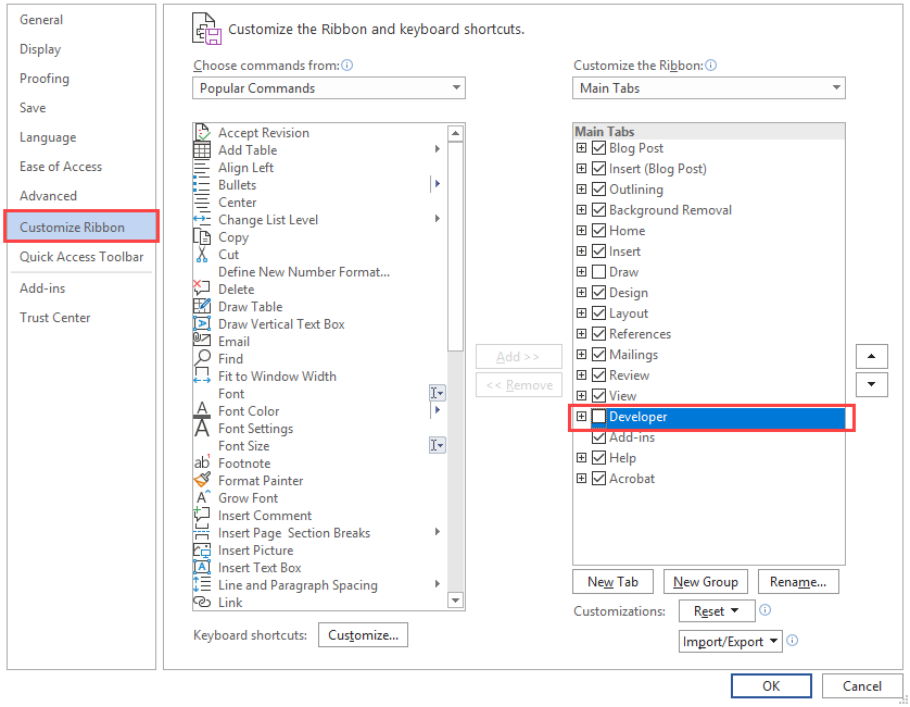
The following section highlights how to work with Content Controls. For more detailed information on these controls, refer to About content controls.

6.10.1.1.1. Content Controls

These controls are managed from the Developer tab in Microsoft Word. This tab isn't displayed by default.

To add the Developer tab to the ribbon:

1. Open Microsoft Word, and on the File tab, go to **Options** > **Customize Ribbon**.
2. Under **Customize** in the Ribbon and under Main Tabs, select the **Developer** check box.



After you show the tab, the Developer tab stays visible, unless you clear the check box or have to reinstall Microsoft Office.

Supported Content Controls

The following five types of Content Controls are supported.

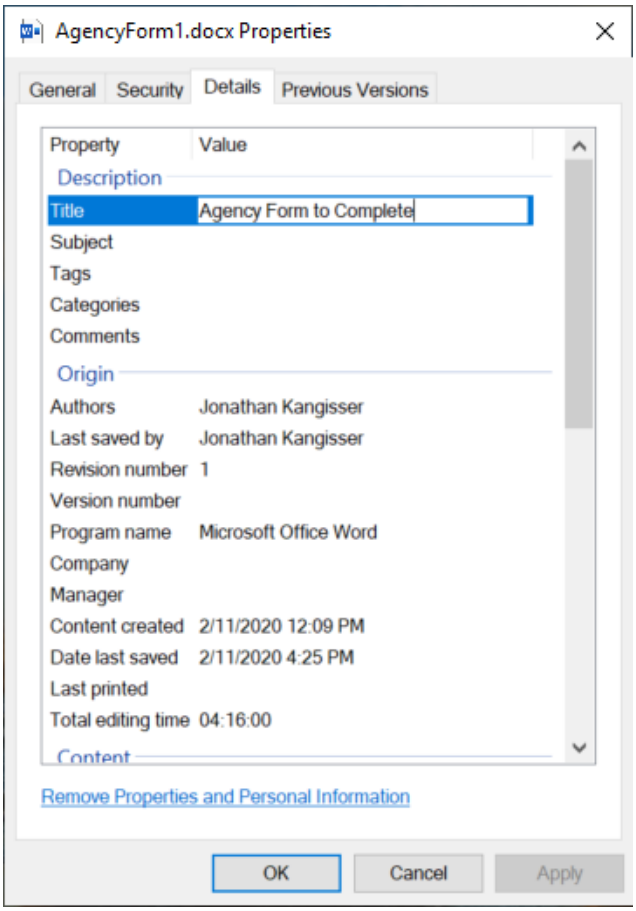
- **Rich Text Content** : Format text as bold or italic, and they can type multiple paragraphs.
- **Plain Text Content** : Insert the plain text content control to limit what users add.
- **Picture** : Add a signature place holder. Every form must have at least one signature. The picture must not be too small.
- **Check Box** : Insert a check box to make the options easier to read and answer.
- **Calendar** : Add a date-time picker that the user can select.

Adding a title to the form

You must add a title to the form. You can add a title in Windows or the Word document.

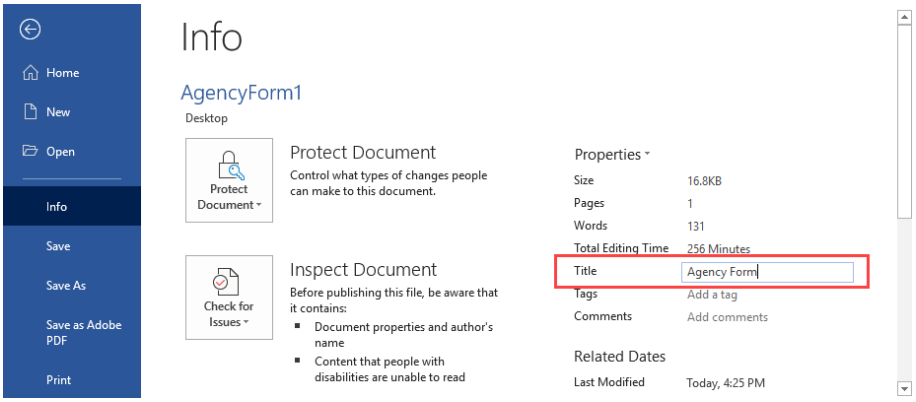
To add a title in Windows:

- Right-click the file name and in the **Details** tab enter the title in the Title field.



To add a title in Word:

» Select **File** > **Info** and enter a title in the Title field.



6.10.1.1.2. Text controls

Adding a text control:

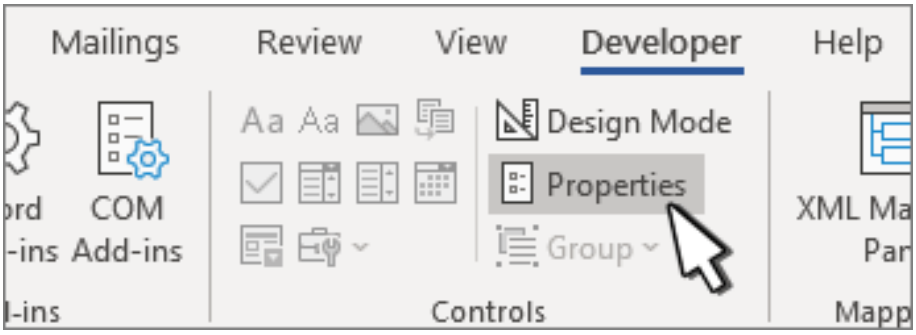
If you want to limit what users add, insert the plain text content control. Click where you want to insert the control. On the Developer tab, in the Controls group, click Rich Text Content Control or Plain Text Content Control .

6.10.1.1.3. Setting properties

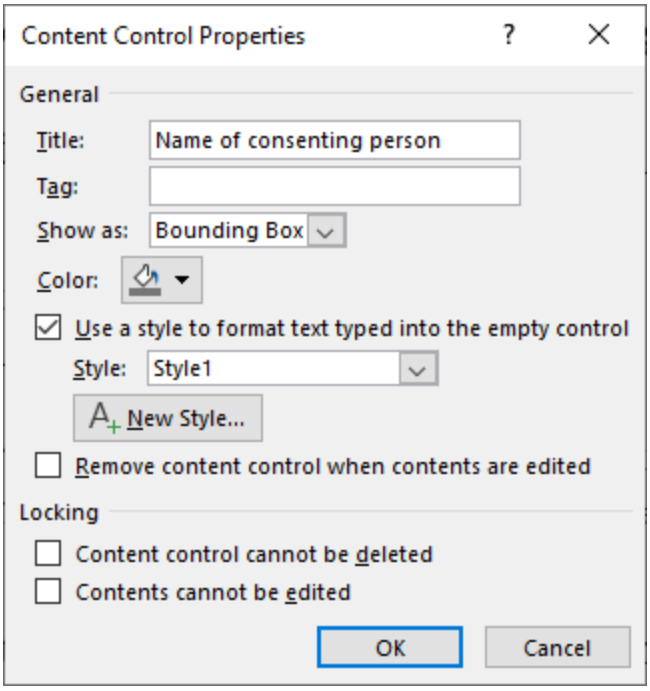
Each content control has properties that you can set or change. For example, the Date Picker control offers options for the format you want to use to display the date.

To set or change properties for content controls:

1. Select the content control that you want to change.
2. Go to **Developer** > **Properties**.



The following window appears.



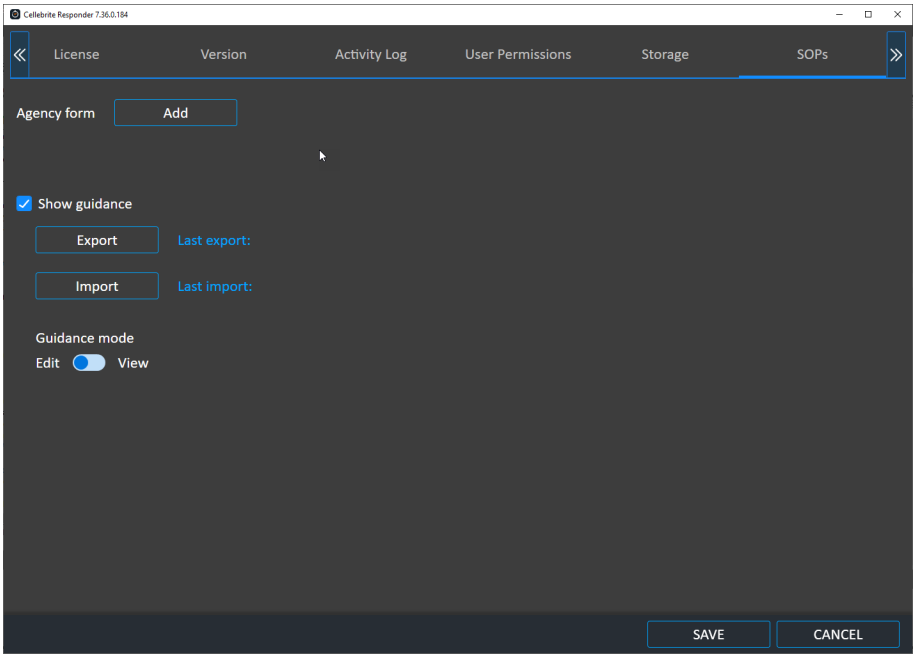
3. Enter a title for the control.

You must enter a title for every content control in the form.

If you provide the same name for two controls in a form, UFED will only asked the user enter the field once.

6.10.2. Workflow guidance settings

Manage Workflow guidance settings in **Settings > SOPs**.



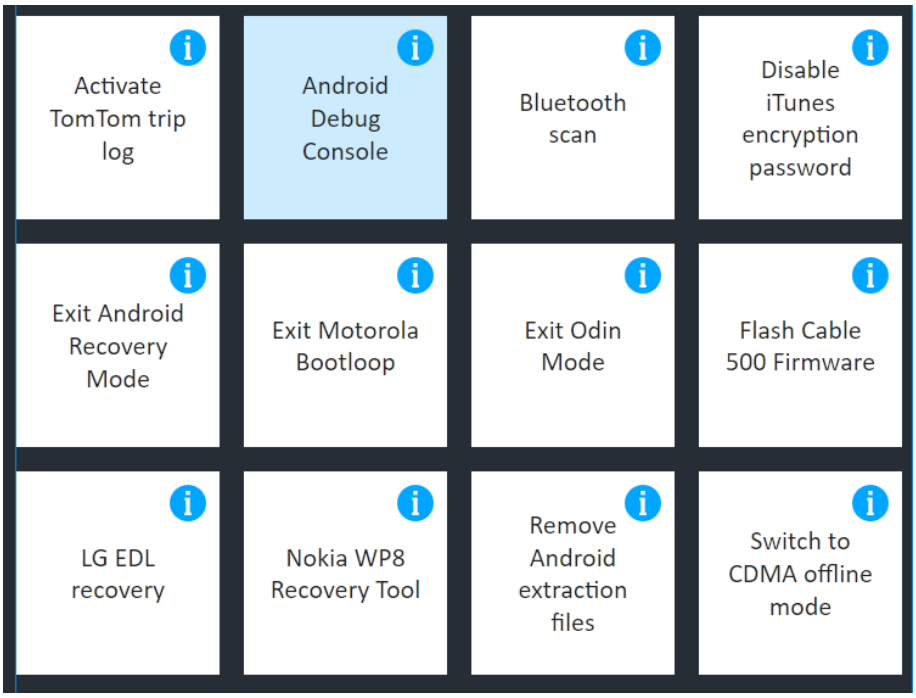
The following settings can be found in the Workflow guidance settings:

- **Show guidance** - When selected, the guidance will appear in the system. Unselect this option to disable the guidance.
- **Export** - Export guidance to be used in other UFED units.
- **Import** - Import guidance file.
- **Guidance mode** - Set the unit to work in either Edit or View mode.

7. Device tools

To access the device tools:

» From the Home screen, tap **Device tools**. The following window appears.



The **Device Tools** screen provides access to the following tools:

7.1. Activate TomTom trip log

This tool enables you to activate or deactivate the trip log logging feature of a connected TomTom device, which is often disabled by the user.

To Activate the TomTom trip log:

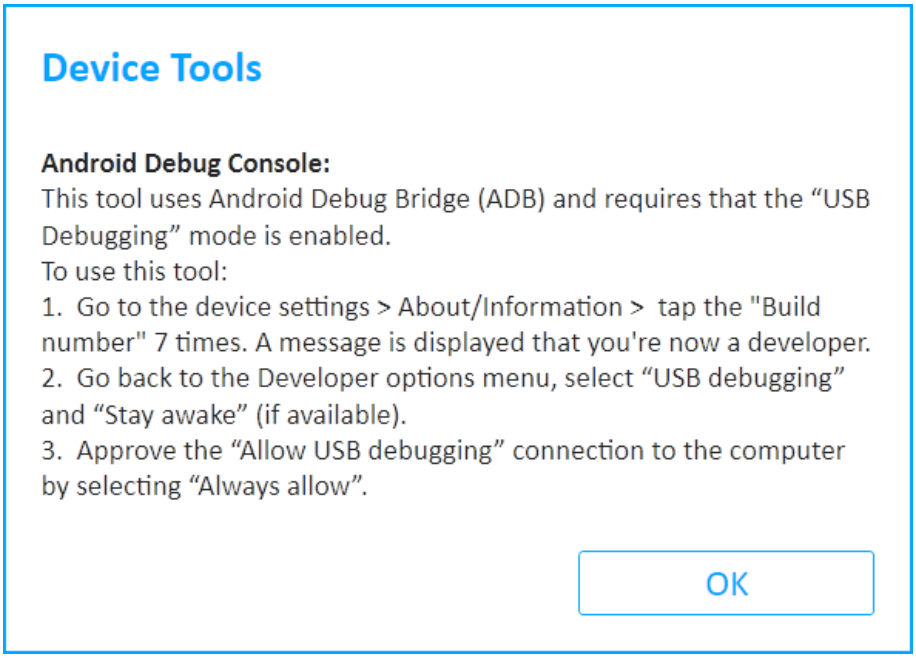
1. Tap **Device tools** and then tap **Activate TomTom trip log**.
2. Connect the UFED Device Adapter (non-kiosk platforms only). The **Select Mode** prompt appears.
3. Select the desired mode. A prompt labeled **Attention** appears requesting to connect the device to the PC.
4. Connect the device to the kiosk or to a USB port on the computer.
5. Tap **Continue**.

7.2. Android Debug Console

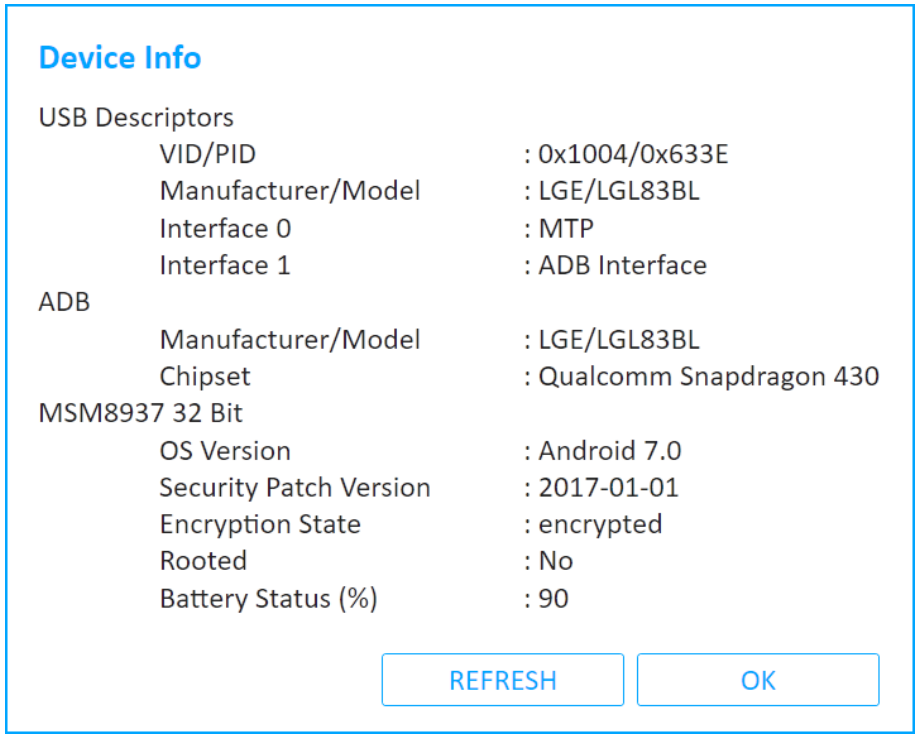
This tool retrieves device information using Android Debug Bridge (ADB).

To use the tool:

1. Tap **Tools** and then tap **Android Debug Console**.
2. If required, you will be prompted to connect the Cellebrite UFED Device Adapter to a USB port (4PC and non-kiosk platforms only). The following window appears.



3. Follow the on-screen instructions.
4. Tap **OK** to receive the device information. The following window appears.

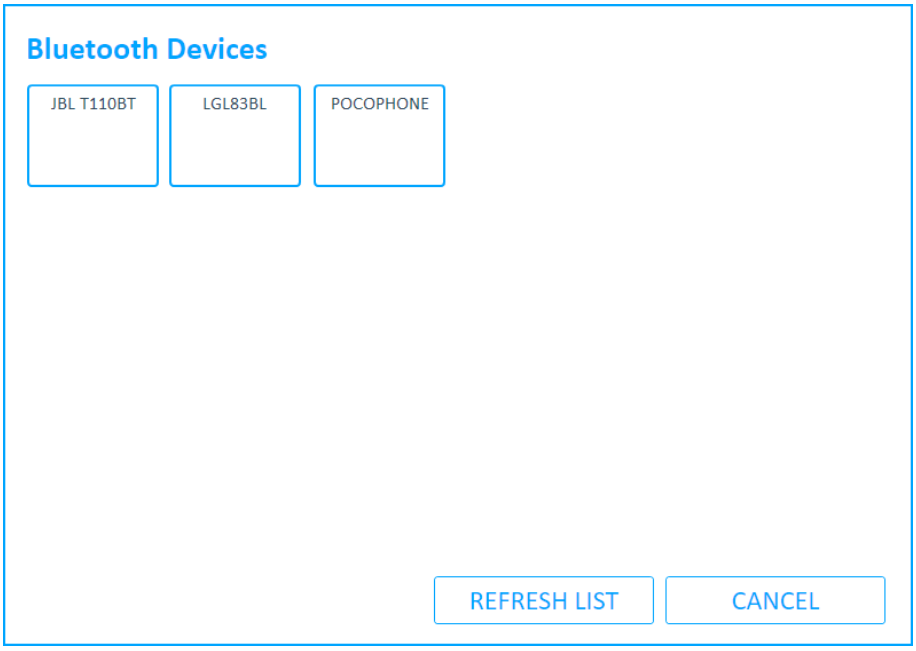

Device Info
USB Descriptors
VID/PID : 0x1004/0x633E
Manufacturer/Model : LGE/LGL83BL
Interface 0 : MTP
Interface 1 : ADB Interface
ADB
Manufacturer/Model : LGE/LGL83BL
Chipset : Qualcomm Snapdragon 430
MSM8937 32 Bit
OS Version : Android 7.0
Security Patch Version : 2017-01-01
Encryption State : encrypted
Rooted : No
Battery Status (%) : 90
REFRESH
OK

7.3. Bluetooth scan

This tool enables you to scan for available Bluetooth devices in your proximity and to pair with them. Make sure that Bluetooth is enabled on the device.

To perform a Bluetooth scan:

1. Tap **tools** and then tap **Bluetooth scan**.
2. Connect the Cellebrite UFED Device Adapter (4PC and non-kiosk platforms only).
3. A list of Bluetooth devices in the vicinity appears. Select one or the following options:
   - Tap one of the devices: The Device summary window appears.
   - Tap **Continue:** Device summary window appears
   - Tap **Refresh list:** Device tool in progress window appears and Cellebrite Responder tries to find additional devices.



7.4. Disable iTunes encryption password

If you select to enable backup encryption during an iOS File system extraction (Full or Backup modes), and for any reason the extraction was stopped in the middle, the device may remain encrypted. This option resets the encryption on the device.

7.5. Exit Android recovery mode

This tool includes two options related to physical extractions using the Forensic Recovery Partition method on Android devices.

- **Exit recovery mode:** In some cases, due to device failure, or if the mobile device was improperly disconnected from Cellebrite UFED, the mobile device remains in recovery mode. This option enables the device to be taken out of recovery mode.
- **Exit bootloop:** In some cases, due to device failure, or if the mobile device was improperly disconnected from Cellebrite UFED, the mobile device keeps rebooting instead of entering the normal mode. This option enables the device to be taken out of this bootloop.

7.6. Exit Motorola Bootloop

In some cases, due to device failure, or if the Motorola mobile device was improperly disconnected from Cellebrite UFED, the mobile device keeps rebooting instead of entering the normal mode. This option enables the device to be taken out of this bootloop.

7.7. Exit Odin mode

To perform physical extractions on some Samsung devices, the device is placed in Odin mode. In some cases, due to device failure, or if the mobile device was improperly disconnected from Cellebrite Responder, the mobile device remains in Odin mode. This option enables the device to be taken out of Odin mode.

7.8. Flash Cable 500 Firmware

When using the Smart ADB method, the firmware on Cable No. 500 is changed and will no longer support the Cellebrite UFED User Lock Code Recovery Tool. The Flash Cable 500 Firmware tool flashes the required firmware to the cable to support either the Smart ADB method or the Cellebrite UFED User Lock Code Recovery Tool.

In the Smart ADB method, Cellebrite UFED verifies the cable firmware and flashes it if required. Cellebrite UFED User Lock Code Recovery Tool does not include cable verification.

To flash the firmware for the Smart ADB extraction method:

1. Tap **Tools** and then tap **Flash Cable 500 Firmware**.
2. Connect the Cellebrite UFED Device Adapter to a USB port (4PC and non-kiosk platforms only).

3. Connect Cable No. 500 (side A) to the USB port.
4. Tap **Smart ADB Firmware** and wait for the process to finish.

7.9. LG EDL recovery

In some cases, due to device failure, or if the mobile device was improperly disconnected from Cellebrite UFED, the LG device remains in emergency download (EDL) mode and appears off. This option enables the device to be taken out of EDL mode.

To use the tool:

1. Tap **Tools** and then tap **LG EDL recovery**.
2. If required, you will be prompted to connect the Cellebrite UFED Device Adapter to a USB port (4PC and non-kiosk platforms only).
3. Follow the on-screen instructions.
4. Tap **Continue** and wait for the tool to finish running.

7.10. Nokia WP8 recovery tool

To perform physical extraction on some Nokia Windows Phone 8 devices, the device is placed in recovery mode. In some cases, due to device failure, or if the mobile device was improperly disconnected from Cellebrite Responder, the mobile device remains in recovery mode. This option enables the device to be taken out of recovery mode.

7.11. Remove Android extraction files

When performing extractions of devices with Android operating systems, a client is installed and some files are written to the mobile device. In some cases (e.g., due to a failure, or if the mobile device was improperly disconnected from Cellebrite Responder) the client and the files remain on the mobile device. This tool uninstalls the client and removes the files from the device.

7.12. Samsung Exynos Recovery

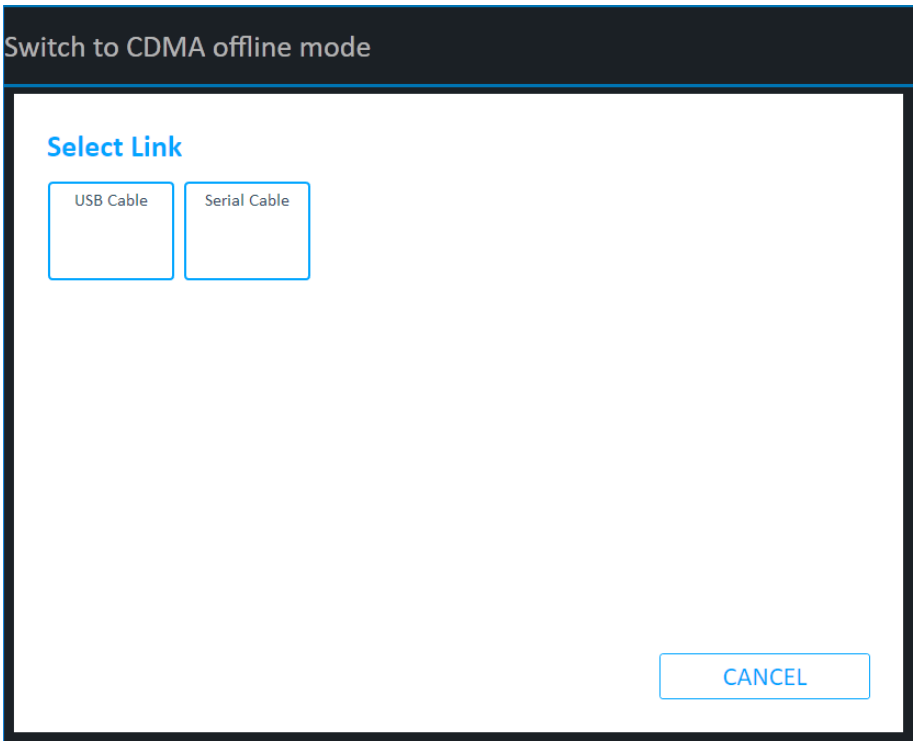
In some cases, due to device failure, or if the mobile device was improperly disconnected from Cellebrite UFED, the device remains off and the Android OS does not start. This option attempts to resolve this issue.

7.13. Switch to CDMA offline mode

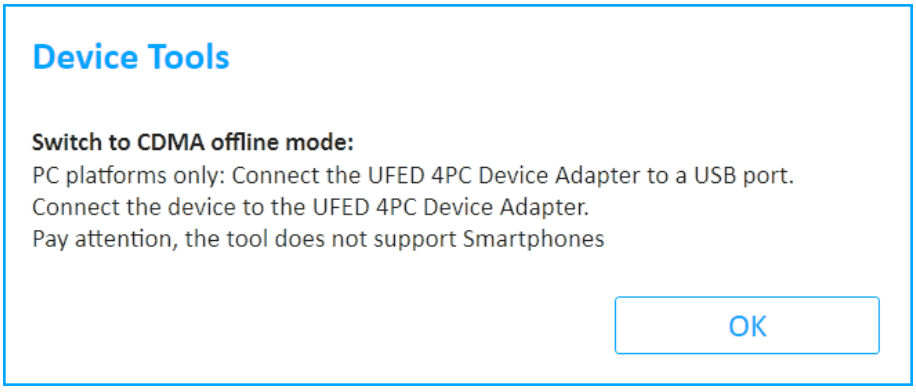
This tool enables you to switch radio on CDMA devices to offline mode.

To switch to CDMA offline mode:

1. Tap **tools** and then tap **Switch to CDMA offline mode**.
2. Connect the Cellebrite UFED Device Adapter (4PC and non-kiosk platforms only). The Select Link prompt appears.



3. Select the link type (**USB Cable** or **Serial Cable**). The Device Tool in Progress window appears.



4. Tap OK.

   Upon completion, the Device Tool Summary appears.

7.14. Uninstall Windows mobile client

To perform logical extractions on devices with Windows Phone operating systems, a client is installed on the device. In some cases, due to a device failure, or if the mobile device was improperly disconnected from Cellebrite Responder, the client remains installed on the mobile device. This option enables the client to be manually uninstalled.

8. Special cables

Cellebrite Responder requires a special cable for certain functions as follows:

Device power-up cable (below)

Active extension cable (on the next page)

USB extension cable (on the next page)

USB cable for Cellebrite UFED Device Adapter V2 PowerUP (on the next page)

8.1. Device power-up cable

In case of a drained or absent battery, the device power-up cable powers the device instead of the battery while performing an extraction.

The device power-up cable contains four parts marked as: Data, Extra power, "-", "+".

Phone power-up cable

To connect the device power-up cable:

1. Connect the Extra Power connector to the Cellebrite Responder USB Port extension.
2. Connect the Data connector to the Cellebrite Responder USB Port extension.
3. Identify the device's battery contacts:
   - Open the device battery cover.
   - Locate the positive ('+') and negative ('–') pole markings of the battery, usually found next to the contacts area.
   - Make sure that the battery contacts are marked clearly on the device's body.
   - Remove the battery in order to gain access to the device's battery contacts.

   TIP: For battery contacts which are not clearly marked on the device's body, use the pole markings on the battery body to identify them. To do that, simply flip the battery along its contacts edge, and place it along the edge of the battery housing, then mark the device's contacts according to those on the battery.

   Use a multi-meter to identify the positive and negative poles of an unmarked battery.

4. Connect the **RED** alligator clip to the device's positive pole ('+'), the Primary **Black** alligator clip to the negative pole ('–') and the secondary **Black** alligator to middle pole in case of three poles or to the one next to the (-) in case of four poles. Make sure the alligator clips are not closing a circuit by touching each other.
5. Connect the source device to the **phone power-up cable** using the references cable from the cable organizer kit as listed in the Cellebrite Responder menu.

8.2. Active extension cable

This cable is 150 cm in length and allows for the easy and accessible placement of the Cellebrite UFED Device Adapter with USB 3.0. For more information on the adapter, see Cellebrite UFED Device Adapter with USB 3.0 (on page 13).

The USB Device Adapter Active extension cable is a custom made, high grade cable with an active USB 3.0 extension. It is a bus-powered extension cable that can be used to increase the length of the Cellebrite UFED Device Adapter without any signal loss or performance issues. It contains active electronics, which boost the USB signal for maximum reliability and performance over extended distances.

The previous USB extension cable i.e., "USB Extension cable for Cellebrite UFED Device Adapter" cable should only be used with the Cellebrite UFED Device Adapter with USB 2.0.

8.3. USB extension cable

This USB extension cable is 150cm in length and will allow for the easy and accessible placement of the Cellebrite UFED Device Adapter V2. In a desktop environment where the computer is mounted in a difficult to access or distant location the USB Extension cable should be used.

The USB Extension cable is a custom made high grade cable. This high grade cable prevents voltage fluctuation and is shielded from EMI interference which would cause signal degradation or loss.

If an extension cable is needed it is **essential** that the provided USB Extension cable is used. Use of third-party cables will affect performance of your Cellebrite Responder and may prevent some functions from starting or completing.

8.4. USB cable for Cellebrite UFED Device Adapter V2 PowerUP

The following USB PowerUP cables are applicable to the Cellebrite UFED Device Adapter V2. These cables are **no longer required** with the

Cellebrite UFED Device Adapter V3.

- The **USB Cable for Cellebrite UFED Device Adapter PowerUP S** for use with your Cellebrite Responder. It is 75cm in length.
- The **USB Cable for Cellebrite UFED Device Adapter PowerUP L** for use with your Cellebrite Responder. It is 150cm in length.

Both cables provide the same functionality and differ only in length.

The PowerUP cable has a miniUSB male end which will plug into the Cellebrite UFED Device Adapter V2 and a USB-A connector which can be plugged into any available powered USB port - including A/C powered USB chargers and car chargers.

The PowerUP cable will double the power capacity of the Cellebrite UFED Device Adapter V2. This will ensure that all devices with excess power requirements will function correctly and will allow Cellebrite Responder to provide all functions. In addition devices that are fully discharged may need the additional power that the PowerUp cable will provide.

In the laptop environment it is recommended that the PowerUp cable is used when Cellebrite Responder indicates that the extra power is needed.

The PowerUp cable is NOT required for smooth operation of the Cellebrite Responder for most devices, but is provided for those cases where power consumption is above the capacity of the unpowered Cellebrite UFED Device Adapter V2.

9. Ordering cables and accessories

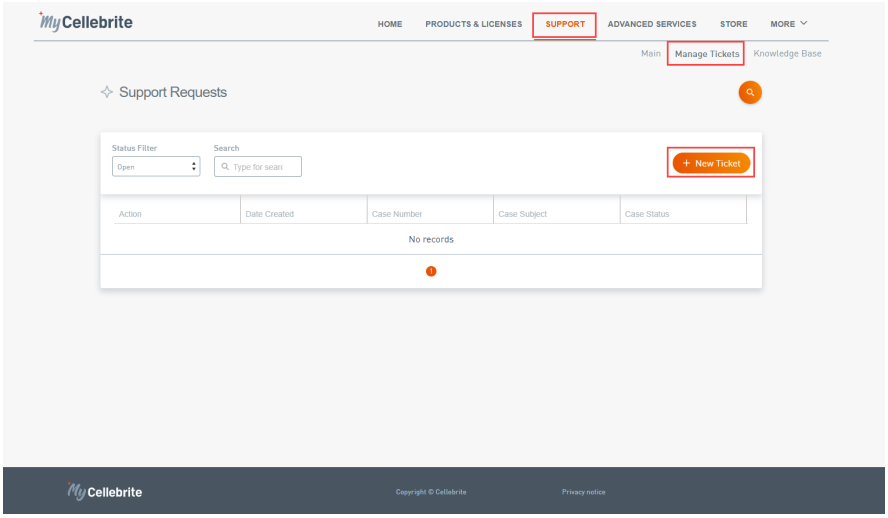
If you have a valid Cellebrite Responder license, it is possible to request missing cables and accessories in the MyCellebrite portal.

Customers can request up to two cables from each cable type per year at no charge.

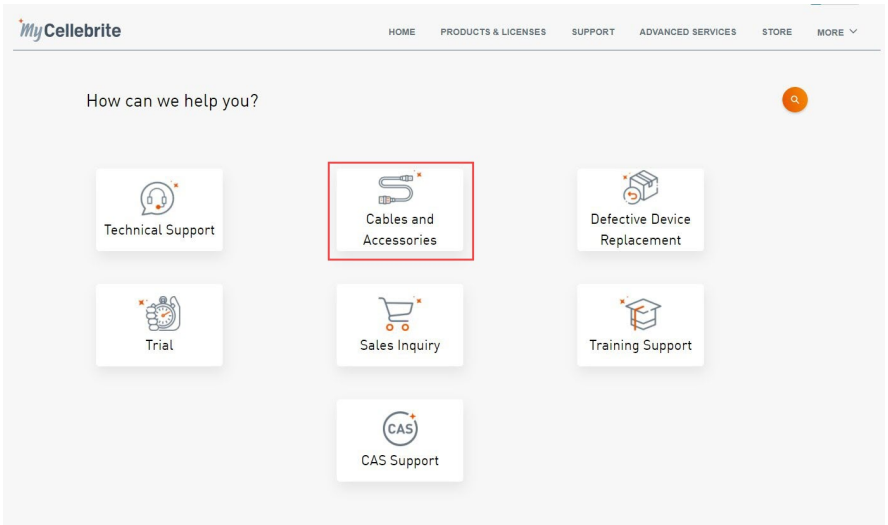
Once ordered, you will receive a confirmation that your request has been accepted, and a notification when shipped.

To order cables and accessories:

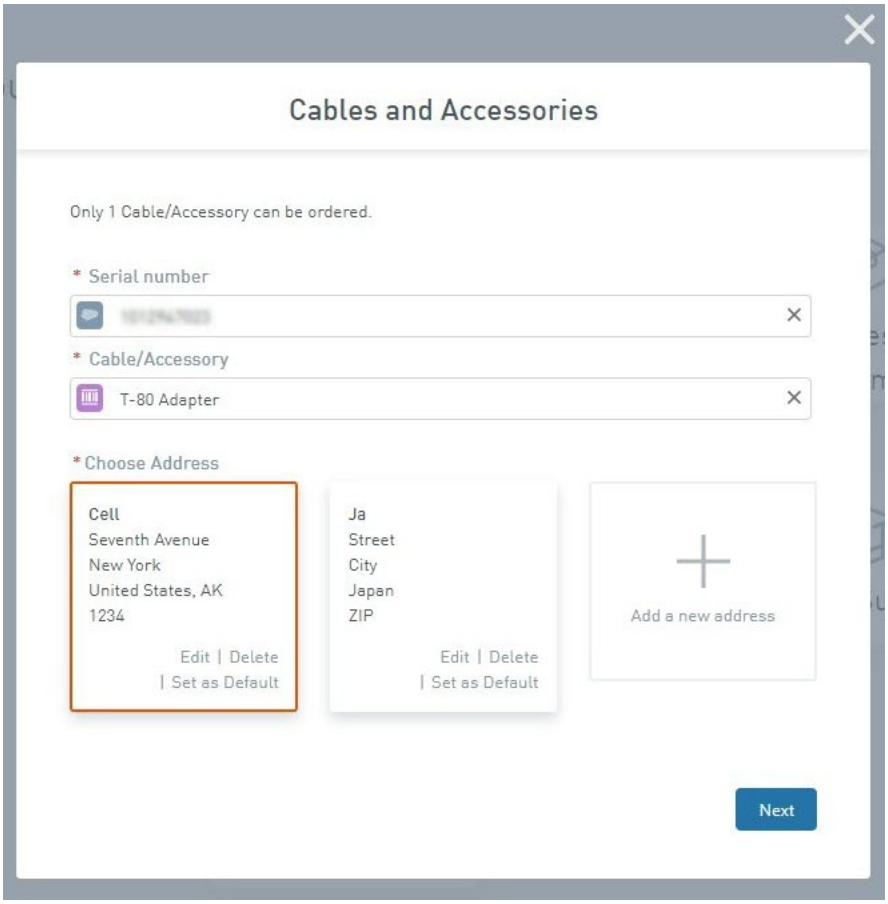
1. Go to the MyCellebrite portal.
2. Navigate to **Support > Manage Tickets**.
3. Click **+ New Ticket**.



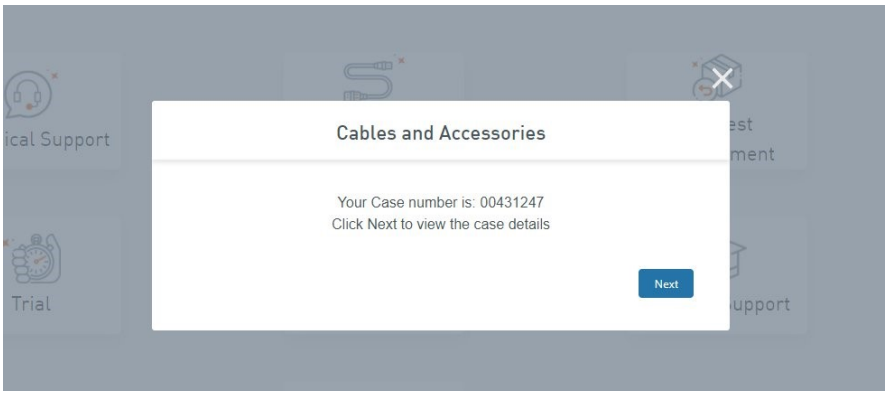
4. Click **Cables & Accessories**.



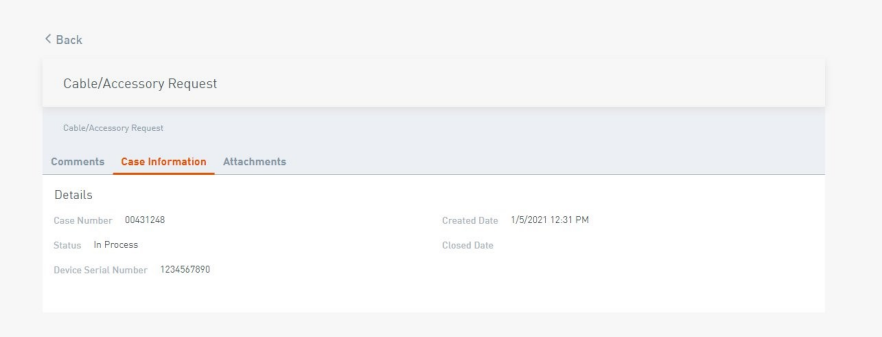
5. Enter the serial number for the product.
6. Select the cable or accessory.
7. Select or add a new address.
8. Click **Next**.



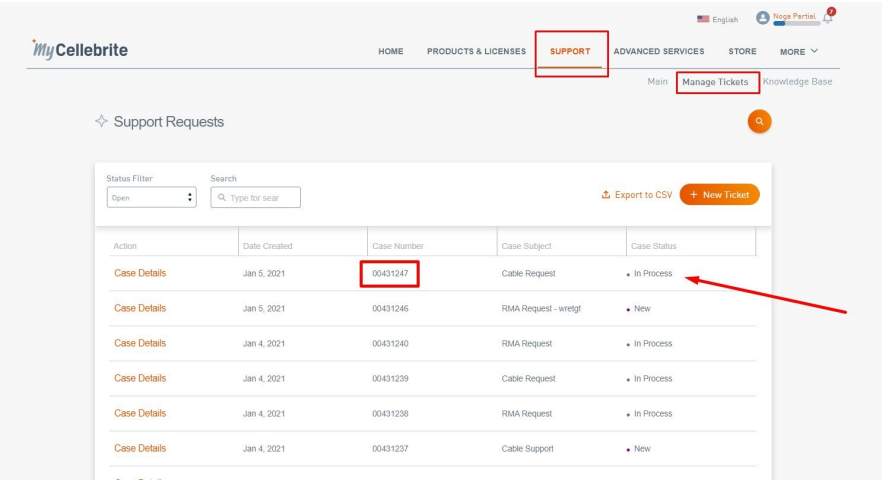
9. Click **Next.**



10. The case details are displayed.



11. Once the cables are shipped you will receive an email notification with the tracking number.
12. You can view the case and its status any time in the MyCellebrite portal by going to **Support > Manage Tickets:**



10. Regulatory compliance

FCC warnings:

This kiosk complies with part 15 of the FCC rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

Standards compliance

CE	
EMC	EN 55032 EN 55024, EN61000-3-2, EN61000-3-3
Safety	EN 60950-1
Radio	EN 300 328 V2.1.2
EMF Exposure	EN62311
FCC	
EMC	FCC part 15, subpart B
Radio	FCC part 15 C

Environment

Temperature and humidity	
Operating	0~40°C
Storage	-20~60°C
Humidity	10~90%

The unit is intended for TN and TT power supply systems and for IT power supply system of Norway only.

In **Finland**: "Laite on liitettävä suojakoskettimilla varustettuun pistorasiaan"
In **Norway**: “Apparatet må tilkoples jordet stikkontakt”
In **Sweden**: “Apparaten skall anslutas till jordat uttag”

11. Specifications: Cellebrite UFED Device Adapter

The specifications for the UFED Device Adapter with USB 3.0 are subject to change without notice.

Item	Properties
Power	USB Powered Optional additional power connection from external 5.3V power supply
Dimensions	67.9mm (D) x 115.8mm (W) x 24.6mm (H)
Weight	200 g
Bluetooth	V2.1+EDR (Backward compatible with V1.1/V1.2/V2.0)
USB	Device: 1 x USB 3.0 **Connection type** / **Power capabilities** USB2.0 single port — 300 mA USB2.0 dual port — 800 mA USB3.0 single port — 600 mA USB3.0 dual port — 900 mA External Power Supply — 2800 mA Host Interface: 1 x USB 3.0 port
Serial ports	RJ-45 for device connectivity
Environmental	Operating temperature: 0°C – 40°C Storage temperature: -20°C – 60°C

Item	Properties	
Regulatory compliance	**Part**	**Description**
	CE	This device complies with the essential requirements of **RED Directive** 2014/53/EU 2014/35/EU 2014/30/EU
	EMC	Following standards: EN 301 489-1 EN 301 489-17 EN 55024
	Safety	IEC/EN 60950-1, CB Scheme
	Radio frequency spectrum usage	EN 300 328
	FCC	
	EMC	FCC part 15, subpart B
	Radio	FCC part 15.247

12. Glossary

A

Active extension cable

This cable is 150 cm in length and allows for the easy and accessible placement of the UFED Device Adapter with USB 3.0.

ADB

Refers to an extraction method most commonly used for file system extractions. ADB, AKA Android Debug Bridge, is a built-in communication mechanism originally designed for device debugging. To enable the device extraction, ADB must be turned on.

ADB (Rooted)

When extracting a rooted device, the operating system version is not a limitation and the extraction can be completed on any Android version.

Advanced ADB

Refers to a physical extraction method, where ADB is used to facilitate the extraction. This method is available for Android OS versions created before December 2016. Depending on the device, this extraction may perform faster than other extraction methods, but takes considerably longer than other extraction methods. With this extraction type, the source device will continue the extraction, once the appropriate commands are sent to the device, with the output directed towards a USB mass storage device (via OTG cable) or SD memory card.

Advanced ADB (Generic)

This process is similar to the ADVANCED ADB mentioned however it is not verified for use on a specific device. It has however been shown to be successful on many

similar devices. In some rare cases, it may not perform as expected, therefore, we recommend trying other extraction types first.

Advanced logical extraction

An extraction method that combines both the logical and file system extractions into a single extraction method. This method helps users overcome the pain of long and convoluted extractions, saving time and effort while maintaining forensically sound data.

Airplane mode

Flight mode, Offline mode, or Standalone mode is a setting that when activated it disables all voice, text, telephone, and other signal-transmitting technologies such as Wi-Fi and Bluetooth. Wi-Fi and Bluetooth can be enabled separately even while the device is in airplane mode.

Allocated space

The area on a device's memory that stores data in an organized manner, and contains its operating system and user data. Logical extractions obtain data from allocated space only.

Android Backup

Supports Android devices running OS version 4.1 and later. It typically provides less data than a regular "ADB" backup, however, depending on the make, model and OS version of the device, it may be the only option available or can be used when the ADB option exists, but is not successful.

Android Backup APK Downgrade extraction

This method focuses on specifically supported apps for decoding. It should be used as a last resort method as data alteration will occur during this process. This method temporarily downgrades the updated version of the app on the device and installs the latest supported version of the app that it can decode.

apk

Android application package file. Each Android application is compiled and packaged in a single file that includes all of the application's code (.dex files), resources, assets, and manifest file.

Apple File Conduit

AFC2. A service that is used by computer applications such as iTunes and iPhoto to read files from a device over USB.

B

Boot loader

A small piece of code that is inserted into the RAM during start-up. In the commercial wireless world, this allows flashing of firmware. In the forensic world, it allows a non-intrusive means of accessing and copying user data into a forensic image.

Brick

A device that cannot function in any capacity (such as a device with damaged firmware).

Bruteforce

Refers to an unlocking technique that relies on trial and error. Combinations are attempted until the correct password or PIN is found.

C

CAS

Cellebrite Advanced Services (CAS) offers customers the ability to recover valuable evidence from heavily damaged, locked or encrypted devices.

CDMA

Code Division Multiple Access. These networks connect using different methods to allow multiple callers access to single voice radio waves, hence Code and Time Division. True CDMA networks do not require handsets to have a SIM card, as the network connects to the device and the subscriber details are contained in the handset rather than a SIM card.

Cellebrite Commander

Simplify how you manage and control all deployed devices and systems with the Cellebrite Commander. Reduce ongoing administration costs by remotely accessing devices and systems across your operation.

Cellebrite Kiosk

The Cellebrite Kiosk "all-in-one" mobile forensic solution is capable of selective data extraction types and decodes mobile device data

Cellebrite UFED 4PC

Enables users to deploy extraction capabilities on Windows based tablets, laptops, and desktop computer systems. It performs physical, logical, file system and password extractions on a wide range of devices.

Cellebrite UFED Touch

Enables the simplified extraction of mobile device data. Depending on the license purchased, it performs physical, logical, file system and password extractions on a wide range of devices.

Chip-off

Otain data straight from the mobile device's memory chip.The chip is detached from the device and a chip reader or a second device is used to extract data stored on the device under investigation.

Client

A client is used during some extractions (usually Logical extraction). It is a very small application that is temporarily installed on a limited number of Android, older Windows Mobile, Palm OS, and Symbian models. The client is unlike a boot loader in that, rather than be installed to the device RAM, it acts like any other third-party app by installing to the device ROM. It does not overwrite any data; it will not install, for example, on a device whose memory is full. It provides enough access to the device's file system that allows UFED to index the file system and determine how many files exist, then extract the data. It is automatically removed from the device afterthe extraction completes. Users are encouraged to document when the UFED prompts them to use the client, and whether they proceed with the extraction.

D

Decrypting Bootloader

This process is designed for Android devices that have Qualcomm chipsets. This extraction can be performed when the device is in Bootloader mode. Bootloader extractions do not support extractions from a memory card or SIM card.

Device power-up cable

In case of a drained or absent battery, the device power-up cable powers the device instead of the battery while performing an extraction. The device power-up cable contains four parts marked as: Data, Extra power, "-", "+".

Dongle license

Is a software copy protection device that plugs into the USB port of the computer. Upon startup, the application looks for the key and will run only if the key contains the appropriate code.

E

EDL (Emergency Download)

Included in the cable or tip set received with your UFED, is an EDL cable. The EDL method is sometimes a superior alternative to advanced techniques, such as JTAG, ISP and Chip-off as they typically can be accomplished without advanced or invasive techniques. It's also possible to use this method on devices that do not function due to damage.

Extraction

The process of obtaining mobile device data and storing it in an approved location for processing.

F

Facelock

Uses an image of the user captured by the front camera to unlock the device. There must be some movement in the face when unlocking the device, to prevent someone from using a still photo to gain access.

File system extraction

Obtains files embedded in the memory of a mobile device. Retrieve the artifacts within a Logical extraction, in addition to hidden system files, databases and other files which were not visible within a logical extraction.

Fingerprint

Newer devices have a fingerprint sensor built into the home button. The user places their finger upon the sensor to gain access to the device.

Forensic Recovery Partition

This extraction method will perform a physical extraction while the device is in Recovery mode. With this extraction method, the original recovery partition is

replaced with Cellebrite's custom forensic recovery partition. Using Cellebrite's custom forensic recovery partition does not affect any of the user data, is forensically sound, and will bypass the user lock from a number of Samsung Android devices.

Forensically sound

Extracted data is said to be forensically sound if it was collected, analyzed, handled, and stored in a manner that is acceptable by the law, and there is reasonable evidence to prove so. Forensic soundness provides reasonable assurance that extracted data was not corrupted or destroyed during investigative processes, whether on purpose or by accident.

I

ICCID

Integrated Circuit Card Identifier. GSM identifier

IMEI

International Mobile Equipment Identifier. GSM identifier

IMSI

International Mobile Subscriber Identity. GSM identifier

Iris scan

Different from retina scans, an iris scan is a form of biometric identification using iris pattern-recognition techniques. The owner of the device establishes the security feature by video scanning the complex, unique but stable patterns of the eye portion surrounding the pupil.

J

Jailbreaking

A jailbroken iOS device or a rooted Android device is one whose owner has taken steps to bypass its factory settings, including built-in security and other restrictions.

Jailbreaking an iOS device allows the user to install third-party apps from sources other than the App Store, while rooting an Android device provides administrative "root" access to its operating system. UFED solutions do not rely on jailbreaking or permanent rooting to perform forensic extractions, as other mobile forensic tools do.

K

Knock pattern

The user taps certain locations on the screen in a certain order to gain access to the device.

L

Logical extraction

Extracts user data from a mobile device (SMS, call logs, pictures, phonebook, videos, audio, certain application data, and more). Quickest extraction method but least amount of data.

M

Markers

Markers signify the location where a person's device registered. The color of the marker signifies which person was registered at a particular location. At a low zoom level, markers show the approximate location, and may include the data of more than one person.

MEID

Mobile Equipment Identity (MEID) is the CDMA equivalent of the International Mobile Equipment Identifier (IMEI) for Global System for Mobile communications (GSM) handsets and is often referred to as the serial number of the handset.

MIN

Mobile ID Number (MIN) is often compared to the International Mobile Subscriber Identity (IMSI) found associated to GSM handsets. The MIN is the number which identifies the subscriber to the CDMA network provider.

MSISDN

Mobile Station International Subscriber Dialing Number. GSM identifier.

MultiSIM Adapter

Is a small-size adaptor which enables reading, data extraction and cloning Nano SIM, Micro SIM and SIM cards.

P

Password Lock/Bypass

Users of devices are routinely secure their data with the user of password locks and security measures. The bypassing or discovery of these security measures largely depends on the make and model of the device as well as the operating system that is in use. Using Cellebrite's extraction technology, some devices are able to have bypasses, where a series of specialized cables and instructions are supplied to either bypass or defeat a security mechanism used. In other cases, instructions will be provided which will allow the user to have the PIN/PASSCODE displayed on the screen.

Physical extraction

The most comprehensive extraction and forensically sound. It uses advanced methods to extract a physical bit-for-bit image of the flash memory of a device, including the unallocated space. Unallocated space is the area of the flash memory that is no longer tracked by the file system. Unallocated space may contain images, videos, files, and more.

Physical/Logical Analyzer

An analysis and reporting tool for logical, file system and physical extractions. This software solution provides users with the capability to extract data, perform advanced analysis, decoding and reporting and presenting the results in a clear and concise manner.

PIN/Password and Pattern Lock

All of the above locks require a secondary lock such as a PIN, password, or pattern lock. Also, a user may select one of these as the primary screen lock for their device.

R

Root

A process that allows users of cell phones and other devices running the Android operating system to attain privileged control (known as "root access") within Android's Linux subsystem, similar to jailbreaking on Apple devices running the iOS operating system, overcoming limitations that the carriers and manufacturers put on such devices.

S

Selective extraction

Performs fast and focused extractions. Pick and choose the applications in which you suspect contains relevant data or leads, and perform a Selective extraction rather waiting several hours for a full file system extraction.

Smart ADB

This method is designed for Android devices that include the “November 2016” security patch. It is supported by OTG compatible devices with OS versions 6.0 and above. Only security unlocked devices are supported.

Smart location

Trusted locations leave the device unlocked for up to four hours when it is turned on, and the device is connected to a secured Wi-Fi access point, trusted Bluetooth device, trusted NFC tag, or if the device detects body movement.

T

TAC

The Type Allocation Code (TAC) is the initial eight-digit portion of the 15-digit IMEI and 16-digit IMEISV codes used to uniquely identify wireless devices. The Type Allocation Code identifies a particular model (and often revision) of wireless telephone for use on a GSM, UMTS or other IMEI-employing wireless network.

U

UFD

Once logical, file system, and physical extractions are complete, UFED generates an extraction file, along with a .UFD (text) file. The .UFD file contains information about the extraction, such as which UFED was used (including its serial number); start time, finish time, and date; and hash information. With iOS physical extractions, the .UFD file also contains decryption keys. For binary images, it may contain some information to aid the decoding process.

UFDR

Universal Forensic Extraction Device Report

UFDX

UFED generates a UFDX file when there are multiple extractions for a device. It contains information about each extraction

UFED

Universal Forensic Extraction Device

UFED CHINEX

The UFED Chinex kit, is the solution to complete a physical extraction, decoding of evidentiary data and passwords from mobile devices manufactured with Chinese chipsets; including MTK and Spectrum.

UFED Memory Card Reader

A multi-format card reader that provides either read-only or read-write access to a variety of flash media cards.

V

Voice lock

The user speaks while unlocking the device, and their voice gains access.

13. Index

T

U

V

W